

Privacy and Security Enforcement Tracker 2017

Published May 2018





<i>Foreword</i>	<i>II</i>
<i>Introduction</i>	<i>IV</i>
<i>Summary Statistics</i>	<i>VI</i>
<i>UK Enforcements</i>	<i>VIII</i>
<i>UK Enforcement Notices</i>	<i>01</i>
<i>UK Monetary Penalty Notices</i>	<i>09</i>
<i>UK Prosecutions</i>	<i>54</i>
<i>UK Undertakings</i>	<i>58</i>
<i>International Trends – Europe</i>	<i>74</i>
<i>International Trends – Rest of World</i>	<i>107</i>
<i>Team and Contact Information</i>	<i>152</i>



If you are looking for more help:

- Visit our website: <http://www.pwc.co.uk/gdpr>
- Visit our blog: http://pwc.blogs.com/data_protection/
- Attend our Data Protection Bootcamps
- Access our Data Protection material

Please contact DP_Enquiries@uk.pwc.com or any other member of the team

Foreword

The publication of PwC's report coincides with the beginning of a new era in data protection. The General Data Protection Regulation, which comes into effect on 25 May 2018, raises the standard of data protection and brings it into the 21st century.

Organisations, as the custodians of personal data, will have to meet the higher thresholds of transparency and accountability that the GDPR demands.

Here at the ICO we'll have greater powers to take enforcement action against those organisations that fall short.

The ICO receives 20,000 complaints from the public a year and another 3,000 incidents are self-reported by organisations. People also tell us about nuisance calls, texts and emails through our online reporting tool. But, as the summary statistics in this report clearly show, only a small proportion lead to formal enforcement action.

And while the new law strengthens our fining powers – from a maximum of £500,000 to £17 million or 4% of global turnover – our approach to enforcement action will not change. We remain committed to the carrot over the stick. Guiding, advising and supporting organisations to help them comply with the law will always be our preference.

We remain a proportionate and pragmatic regulator. Big fines will be reserved for those who wilfully, negligently or consistently flout the law.

But whatever action we take, people will always be at the heart of what we do. Their data matters. It matters to them, it matters to us and it must matter to the organisations looking after it.

James Dipple-Johnstone



James Dipple-Johnstone is Deputy Commissioner (Operations) responsible for the ICO's statutory investigation, audit, complaints handling, Binding Corporate Rules and appeals functions.

James joined the ICO in 2017 from the Solicitors Regulatory Authority (SRA), where he had been Director of Investigation and Supervision leading their teams assessing and investigating reports of professional misconduct, money laundering, cybercrime and fraud involving solicitors and law firms. James's background is in regulatory investigation, appeals and complaints handling.

He has held posts as Commissioner for the Independent Police Complaints Commission, Director of Investigation for the Parliamentary and Health Service Ombudsman and in NHS regulators.

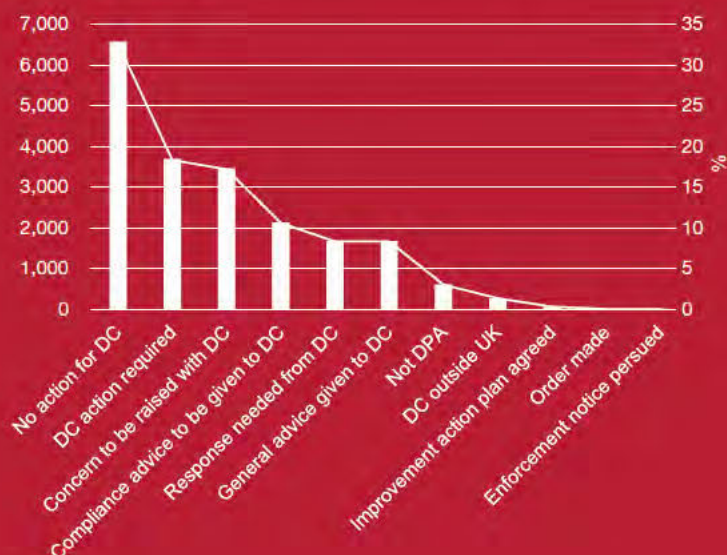
ICO Statistics

Helpline calls received:



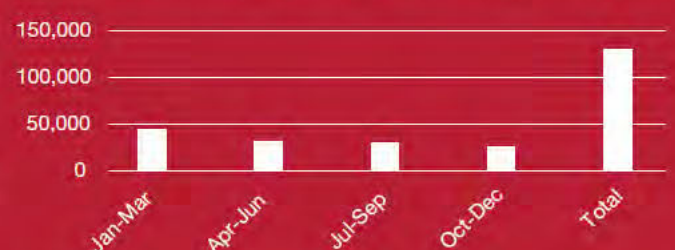
Source: ICO Annual Report and Financial Statements 2010/11 – 2016/17

Outcomes for Data Protection complaints raised in 2017



Source: ICO

Volume of concerns about nuisance calls, texts and emails raised via online tool in 2017



Source: ICO

PwC Privacy and Security Enforcement Tracker 2017

Welcome to the fourth annual PwC Privacy and Security Enforcement Tracker, where we review the key regulatory enforcement cases in the UK and in 34 other countries in 2017.

As GDPR fever took hold in 2017 we saw an explosion in volumes of data protection work all around the PwC global network. Although it seems that every year is dubbed 'a year like no other', with each passing month, as the GDPR shock waves fanned out from Europe to all corners of the world, it seemed like a new reality started to bite. In no time at all the new law would be upon us, leaving everyone in the data processing environment at the mercy of regulators, litigants, angry consumers and disgruntled employees alike!

However, none of us can really be sure about what the future will hold. It might contain prospects of great stress and anxiety for some or perhaps there will be massive fines and more high profile litigation. There is great potential for more high profile privacy news stories about corporate governance failures and Parliamentary inquiries may become a permanent feature of the landscape.

But, there will also be big opportunities for those who embrace the new reality, which is that data protection is here to stay. This topic will continue to grow in importance and we will eventually reach a point whereby bad practices are seen as self-defeating and anti-social. The data controllers and processors that get ahead of this sea-change will win out.

The signs are very encouraging. At Board tables all over the world we are hearing a refreshing new regard for personal data. Business and government leaders are

really starting to 'get it'. Indeed, in the UK right now, in the middle of the Brexit process, there is data protection, an area that both sides have agreed needs special treatment, care and attention. Could you have imagined that just five years ago? Of course not – data protection wasn't even an issue during the 2016 referendum campaigns. We have come a very long way in a short space of time and we are seeing the positive fruits of this change all around us, as businesses, public authorities, government departments, charities, churches and schools proudly publish their new privacy notices and try to improve their consents and permissions. In that sense, the GDPR has already been a great success.

Still we should not forget that the law has to have its red lines. The reason why regulatory law is needed is because there will always be reasons or incentives for people and organisations to take short cuts and to ride rough shod over matters of societal importance. We do not always aspire to do the noble thing. So regulatory law exists to control and change these imperfections, to encourage and steer us more towards the good. And the regulatory offices, the courts and the legal systems of the land are the champions of the good and our last line of defence against those who threaten our liberties, rights and freedoms. All of us have to listen to what the regulators and the courts are saying and take account of their positions. We also need to help them with the performance of their duties, but challenge them strongly if they get things wrong.

This is why the PwC Privacy and Security Enforcement Tracker exists. Our multi-disciplinary team of data protection professionals truly believes that our clients need to keep abreast of and understand developments in the law and factor them into their preparations for the GDPR and their ongoing activities. And while a prudent organisation like ours will never say that the past is guarantor of the future, we are confident that the data protection environment will continue to build upon

its historical foundations and that trends and hot topics that are exposed by the cases are ones that we all need to understand.

The UK

In 2017 the UK Information Commissioner's Office continued its role as one of Europe's leading data protection regulators and despite a massive amount of its effort being dedicated to GDPR preparations, such as the publication of new guidance, the ICO still managed to significantly increase its tally of fines in comparison to 2016, although overall the number of cases that ended in enforcement action was slightly down on the year before. As in 2016, data protection marketing problems were one of the dominant causes of enforcement actions, with almost half of the cases being related to this area. Security breaches continued to appear as a substantial cause of failure, but a standout development was a series of cases against the Charity sector, about wealth screening, which is a profiling activity. The Commissioner also pursued a very high profile investigation into the data analytics industry, with a particular focus on the use of data analytics in political processes, including profiling. So, 2017's cases point to marketing, profiling and security as being the big areas for organisations to be mindful about.

In the litigation environment, the landmark case of 2017 concerned a supermarket's liability to its employees for a security and confidentiality breach caused by a rogue insider, which ended in success for the 'class action', although the case is still under appeal. That case is part of a recent trend of 'class action' cases in the UK, which suggests that this phenomenon is here to stay.

Europe

There were a number of notable enforcement cases in Europe in 2017. For example, in **Germany** a supermarket was fined €1.5m for using private detectives and secrets cameras in its stores, while an insurance company was fined €1.3m due

to buying personal data from government employees. In **Italy** fines totalling €11m were imposed on five companies operating in the money transfer industry, where 1000 people were affected by unlawful data processing.

Another notable feature was the launching of regulatory investigations into high profile cases that appeared in the news. **Ireland** and **Netherlands** are examples of territories that have reported investigations into big technology companies that received bad press in 2017.

Increasing volumes of concluded cases is another feature of 2017 in Europe. For example, in **Belgium** there were 332 inspections, while **Estonia** reports nearly 400 concluded enforcement cases, **Poland** reports over 300 concluded enforcement cases and **Romania** reports that there were 193 fines and 357 sets of undertakings. **Romania** is also the origin of one of the most important court cases in 2017, *Barbulescu v. The Romanian Government*, a European Court of Human Rights case about unlawful workplace monitoring.

The wider world

Of course, data protection law principles do not reside wholly in Europe, or within the narrower geographical zone of the GDPR. They are present worldwide as the contributions from our data protection experts in **China, Japan, Russia** and **South Africa** reveal. In **Argentina**, for example, there was litigation about 'right to be forgotten' principles. In **Australia** a new law on breach reporting came into effect and there was litigation about the nature of metadata. In **Canada** one of the regulators imposed a \$1.1m fine for spamming, although it was eventually reduced on appeal. While **India** does not yet have a data protection law of EU standards, its current legislative framework was used to promote cyber security and breach reporting. **Japan** introduced new legislation that imposed restrictions on cross border data flows and there was 'class action' style litigation

about personal data confidentiality breaches. **Mauritius** introduced a new law to align with the GDPR and **Russia** reported an increase in regulatory actions, including investigations into high profile US tech companies. In other countries, such as **New Zealand, Georgia, Peru, Paraguay** and **Mexico** the legal frameworks continued to develop.

Plainly, the world has not yet reached a common standard of data protection, but the foundation stones and momentum are in place, which encourages us to think that this will be achieved at some point and maybe sooner than we might think. Perhaps this will occur through the actions of private law actors that operate on the global stage and through extended supply chains, or possibly through the court systems, which seem to be permitting data protection related litigation everywhere and conceivably it may even happen through international treaties. However, the immediate challenge faced by our clients is what to do in places where the law is fuzzy and unclear. We believe that the principles of data protection operate universally, if only as a code of practice for good, ethical business and that legal fuzziness by itself does not provide a reason not to act. We see data protection as being in all our clients' interests, irrespective of what the law says.

The United States

If the imposition of fines and penalties and awards of compensation are the measures of data protection legal strength, again, the United States stands tall in comparison to the rest of the world. Our US practice reports that the Federal Trade Commission imposed penalties of approximately \$470m in 2017 for breaches of the FTC Act that would be regarded as data protection breaches in Europe. Other sector regulators imposed an additional \$140m in penalties. Litigation awards reached \$600m. These staggering numbers show the reality of significant data protection failure in the US.

However, the US does not currently provide 'universal' data protection, in the sense that is recognised in Europe and if this is a gap, which may be debatable, we have seen private law actors moving to fill it, through the adoption of GDPR-type measures in their organisations. Indeed, one of the surprising features of PwC's experience of the GDPR is that US head-quartered entities seem to be outspending their European counterparts on GDPR compliance. This leaves us with much food for thought.

The Tracker

This year we have tried to introduce new strands of analysis, which we will build upon in the years ahead. You will see that we have tried to bring forth evidence on litigation and on the progress made in Europe on the adoption of the Cyber Security Directive. We hope this additional information is helpful, but we welcome feedback.

Going digital

This year, we've also created two interactive data tools – one for the UK and one for the rest of the world - allowing you to explore the facts and figures in the enforcement tracker that interest you most, in more detail. Please visit our site at www.pwc.co.uk/gdpr/insights to access these explorers.

Privacy Transformation and MyDPO

Privacy Transformation is PwC's methodology for providing end-to-end support to clients on data protection. To celebrate GDPR-Live, on 25th May 2018 we are launching the next phase of our methodology, which is called MyDPO. MyDPO is our range of services that support our clients' internal data protection frameworks and functions and, of course, their DPOs, if they need to appoint one. MyDPO launches first in the UK and before we roll out into other territories.

For further information about MyDPO, please contact Stewart Room, Fedelma Good or any other member of our team.



Stewart Room

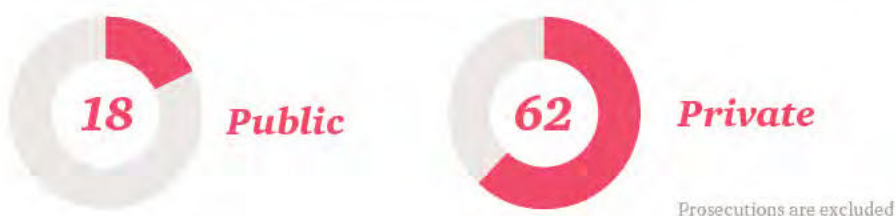
Global Head of Cyber Security and Data Protection Legal Services; UK Data Protection National Lead
+44 (0) 7711 588978
stewart.room@pwc.com

Summary statistics

Enforcement activities: analysis of statistics 2012–2017



Enforcement activities in 2017



Findings from PwC research

Many businesses are still beginners at data-use governance

Only about half of respondents have put key measure in place



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018

Findings from PwC research

Banking and Capital Markets (BCM) CEO's



This year, 82% of BCM CEOs say they are creating transparency in the usage and storage of data as part of their efforts to strengthen consumer trust

93% of BCM CEOs are investing more heavily in cybersecurity

Source: PwC's 21st CEO Survey: key findings from the banking and capital markets industry

Telecoms CEO's



45% of Telecommunication CEOs are extremely concerned about cyber threats* versus 40% for the overall cross industry population

*Cyberattacks are especially serious for telecoms, as these firms handle not only their own data but for a great many other companies and customers

Source: PwC's 21st CEO Survey: key findings from the telecommunications industry



MyDPO

Tailored, accessible and comprehensive support in a GDPR-live environment

PwC's MyDPO service consists of a suite of propositions that have been designed to support clients in the GDPR 'live' environment (25th May 2018 onwards).

Our services are aimed at all businesses, across sectors and geographies who are looking to evaluate, outsource or augment some or all of their data protection activities. The services are categorised in to four themes:

1. Review and assess
2. Strategy and governance
3. Day-to-day support
4. Crisis support

For example:

Review & Assess: Our GDPR Completeness Assessment Tool (C.A.T) will provide you with rapid insight in to your current state of maturity with the provisions of the GDPR, allowing you to make more informed choices over investment and risk management.

Strategy & Governance: Our data protection specialists provide strategic advice to help you optimise your Data Protection Operating Model

Day-to-day Support: Our privacy mailbox outsourcing service helps ensure your customer's queries are responded to quickly and effectively

Crisis Support: Our Personal Data Breach Management Service is staffed by leading experts in data protection crisis and breach management and has been designed to support your business in times of distress and challenge, helping you manage GDPR reporting timescales alongside strategic and operational decision making.

For further information please contact us at DP_Enquiries@uk.pwc.com

UK Enforcements



UK Enforcement Notices

Require organisations to take
(or refrain from taking) specified
steps in order to ensure they
comply with the law

<i>Total</i>	<i>15</i>
Public Sector	<i>2</i>
Private Sector	<i>13</i>

Davies Brothers (Wales) Limited

23 January 2017

DPA — 6th Principle

Davies Brothers (Wales) Limited is a “data controller” as defined in section 1 (1) of the Data Protection Act 1998 (“DPA”).

Section 4 (4) of the DPA provides that, subject to Section 27 (1), it is the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.

The Commissioner held that Davies Brothers (Wales) Limited contravened the Sixth Data Protection Principle in that, contrary to Section 7, it has failed to inform the complainant, without undue delay, whether personal data of which this individual was the data subject were being processed by or on behalf of the data controller and, where that was the case, failed, without undue delay, to have communicated to them in an intelligible form information which may constitute personal data.

Enforced remedial action required within 30 days:

1. Inform the complainant whether the personal data processed by the data controller includes personal data of which the complainant is the data subject and supply them with a copy of any personal data so processed in accordance with the requirements of Section 7 of the DPA and the Sixth Data Protection Principle in that respect, subject only to the proper consideration and application of any exemption from, or modification to, Section 7 of the DPA provided for in or by virtue of part IV of the DPA which may apply.

Road Accident Consult Ltd t/a Media Tactics

3 March 2017

Monetary Penalty

PECR — Regulations 19 & 24

Between 13 November 2014 and 9 June 2015 Media Tactics instigated the transmission of 22,065,627 automated marketing calls to subscribers without their prior consent. Media Tactics also contravened Regulation 24 of PECR in that it did not identify the person who was sending or instigating the automated marketing calls or provide the address of the person or a telephone number on which this person can be reached free of charge.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of communications comprising recorded matter for direct marketing purposes by means of an automated calling system except:
 - a. Where the called line is that of a subscriber who has previously notified Media Tactics that for the time being they consent to such communications being sent by, or at the instigation of, Media Tactics; and
 - b. Where the communication includes the name of Media Tactics and either the address of Media Tactics or a telephone number on which Media Tactics can be reached free of charge.

Munee Hut LLP

10 March 2017

Monetary Penalty

PECR — Regulation 22

Between 1 May 2015 and 22 March 2016, Munee Hut LLP used a public telecommunications service for the purposes of instigating the transmission of approximately 64,000 unsolicited communications by means of electronic mail to individual subscribers for direct marketing purposes contrary to Regulation 22 of PECR.

Enforced remedial action required within 35 days:

1. Except in the circumstances referred to in paragraph (3) of Regulation 22 of the Regulations, neither transmit, nor instigate the transmission of unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient has previously notified Munee Hut LLP that they consent for the time being to such communications being sent by, or at the instigation of Munee Hut LLP.

Types of breach per legislation



2017

PECR breaches: **12**

Data Protection Act (DPA) breaches: **3**

2016

PECR breaches: **12**

Data Protection Act (DPA) breaches: **11**

Xternal Property Renovations Ltd

28 March 2017

Monetary Penalty

PECR — Regulation 21

The Commissioner has received numerous complaints via the TPS and directly from individuals who are subscribers to specific telephone lines. The individuals allege they have received unsolicited marketing calls on those lines from Xternal Property Renovations Ltd. Each individual states that they have previously notified Xternal Property Renovations Ltd that such calls should not be made on that line and/or have registered their number with the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of a public electronic communications service for the purposes of making unsolicited direct marketing calls where the called line is that of:
 - a. A subscriber who has previously notified Xternal Property Renovations Ltd that such calls should not be made on that line; and/or
 - b. A subscriber who has registered their number with the TPS at least 28 days previously and who has not notified Xternal Property Renovations Ltd that they do not object to such calls being made.

Brighter Homes Solutions Ltd

12 May 2017

Monetary Penalty

PECR — Regulation 21

The Commissioner has received 187 complaints via the TPS and directly from individuals who are subscribers to specific telephone lines. The individuals allege they have received unsolicited marketing calls on those lines from Brighter Home Solutions Ltd. Each individual states that they have previously notified Brighter Home Solutions Ltd that such calls should not be made on that line and/or have registered their number with the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of a public electronic communications service for the purposes of making unsolicited direct marketing calls where the called line is that of:
 - a. A subscriber who has previously notified Brighter Home Solutions Ltd that such calls should not be made on that line; and/or
 - b. A subscriber who has registered their number with the TPS at least 28 days previously and who has not notified Brighter Home Solutions Ltd that they do not object to such calls being made.

Concept Car Credit Limited

12 May 2017

Monetary Penalty

PECR — Regulation 22

Over an 18 month period between 2015 and 2016, the Company used a public telecommunications service for the purposes of instigating the transmission of 336,000 unsolicited communications by means of electronic mail to individual subscribers for direct marketing purposes contrary to Regulation 22 of PECR.

In this case the Commissioner is satisfied that the Company did not have the consent, within the meaning of the regulation 22 (2), of the 336,000 subscribers to whom it sent unsolicited direct marketing text messages.

Enforced remedial action required within 35 days:

1. Except in the circumstances referred to in paragraph (3) of Regulation 22 of the Regulations, neither transmit, nor instigate the transmission of unsolicited communications for direct marketing purposes by means of electronic mail unless the recipient has previously notified Concept Car Credit Limited that they consent for the time being to such communications being sent by, or at the instigation of Concept Car Credit Limited.

Medway Council

9 June 2017

No Monetary Penalty

DPA — 7th Principle

The Commissioner's Office carried out a consensual audit of the data controller (Medway Council) in October 2014 which provided 'limited assurance'. The audit report recommended (among other things) that mandatory data protection training should be given to all staff and that there is regular refresher training which is monitored.

The Commissioner's office carried out a 'follow-up' audit in June 2015. Although mandatory data protection training had been implemented, the Commissioner's office advised the data controller to continue to roll out the training. The Commissioner's office carried out a further investigation into the data controller's compliance with the provisions of the DPA following two security breaches. The data controller has failed to take adequate steps to ensure that mandatory data protection training has been rolled out, as advised.

The Commissioner's has considered the data controller's compliance with the provisions of the DPA in light of these matters.

Enforced remedial action required within 6 months:

1. There is a mandatory data protection training programme for staff and refresher training at least every two years. Delivery of the training should be tailored to reflect the needs of the staff following a training needs analysis; and
2. Completion of any such training is monitored and properly documented.

Number of enforcement notices issued per year that resulted in a MPN being issued

2017: **12**

2016: **5**

2015: **1**



H.P.A.S. Limited t/a Safestyle UK

31 July 2017

Monetary Penalty

PECR — Regulation 21

The Commissioner received 264 complaints via the TPS and directly from individuals who are subscribers to specific telephone lines. The individuals alleged that they have received unsolicited marketing calls on those lines from HPAS. Each individual stated that they had previously notified HPAS that such calls should not be made on that line and/or have registered their number with the TPS.

Enforced remedial action required within 70 days:

1. Review all of its telephone marketing data to ensure that it can evidence the consents it relies upon to make marketing calls. Pursuant to the Commissioner's Direct Marketing Guidance the consent must be knowingly and freely given, clear and specific.
2. All such data where the evidence of specific consent cannot be verified, shall be screened against the TPS register before being used to make marketing calls.
3. Put in place an effective suppression system to ensure that all requests not to be called again received from subscribers are recorded, actioned and retained in place until such a time as positive specific consent to receiving such calls is obtained.
4. Screen all unsolicited calls against that suppression system and against the TPS register.

Laura Anderson Limited t/a Virgo Home Improvements

31 July 2017

Monetary Penalty

PECR — Regulation 21

The Commissioner received 440 complaints via the TPS and directly from individuals directly who are subscribers to specific telephone lines. The individuals alleged that they have received unsolicited marketing calls on those lines from Virgo. Each individual stated that they had previously notified Virgo that such calls should not be made on that line and/or have registered their number with the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of a public electronic communications service for the purposes of making unsolicited direct marketing calls where the called line is that of:
 - a. A subscriber who has previously notified Virgo that such calls should not be made on that line;
 - b. A subscriber who has registered their number with the TPS at least 28 days previously and who has not notified Virgo that they do not object to such calls being made.

True Telecom Limited

6 September 2017

Monetary Penalty

PECR — Regulations 21 & 24

The Commissioner received numerous complaints via TPS and directly from individuals who are subscribers to specific telephone lines. The individuals allege that they have received unsolicited marketing calls on those lines from True Telecom. Each individual states they have previously notified True Telecom that such calls should not be made on that line and/or have registered their number with the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of a public electronic communications service for the purposes of making unsolicited direct marketing calls where the called line is that of:
 - a. A subscriber who has previously notified True Telecom that such calls should not be made on that line;
 - b. A subscriber who has registered their number with the TPS at least 28 days previously and who has not notified True Telecom that they do not object to such calls being made.
2. Neither use, nor instigate the use of a public electronic communications service for the purposes of making calls (whether solicited or unsolicited) for direct marketing purposes except where they:
 - a. Do not prevent presentation of the identity of the calling line on the called line; or
 - b. Present the identity of a line on which they can be contacted.
3. In accordance with Regulation 24 of the Regulations, cease using a public communications service for the transmission of a communication to which Regulation 21 of the Regulations applies unless the particulars mentioned in paragraph (2)(a) of Regulation 24 of the Regulations are provided with that communication.

In addition to the above, The Commissioner would note at this point that in the period of May 2017 – July 2017, following the established contravention which forms the basis of this Notice, in excess of 50 further complaints have been logged with the TPS in respect of unsolicited calls made by True Telecom.

Easyleads Limited

14 September 2017

Monetary Penalty

PECR — Regulations 19 & 24

Between 22 October 2015 and 30 June 2017 Easyleads Limited instigated the transmission of 16,730,340 automated marketing calls to subscribers without prior consent, resulting in 551 complaints to the ICO. Easyleads Limited also contravened Regulation 24 of PECR in that it did not identify the person who was sending or instigating the automated marketing calls or provide the address of the person or a telephone number on which this person can be reached free of charge.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of communications comprising recorded matter for direct marketing purposes by means of an automated calling system except:
 - a. Where the line called is that of a subscriber who has previously notified Easyleads Limited that for the time being they consent to such communications being sent by, or at the instigation of, Easyleads Limited; and
 - b. Where the communication includes the name of Easyleads Limited and either the address of Easyleads Limited or a telephone number on which Easyleads Limited can be reached free of charge.

Vanquis Bank Limited

4 October 2017

Monetary Penalty

PECR — Regulation 22

Between 9 April 2015 and 16 February 2016, Vanquis Bank Limited (VBL) used a public telecommunications service for the purposes of instigating the transmission of 870,849 unsolicited communications by means of electronic mail (text message) to individual subscribers for direct marketing purposes contrary to Regulation 22 of PECR. This resulted in 131 complaints being made to the 7726 system.

Furthermore, between 1 April 2016 and 1 September 2016, VBL used a public telecommunications service for the purposes of instigating the transmission of 620,000 unsolicited communications by electronic mail (e-mail) to individual subscribers for direct marketing purposes contrary to Regulation 22 of PECR. This resulted in 9 complaints being made to the ICO.

The Commissioner was satisfied that VBL did not have the consent within the meaning of Regulation 22 (2) from the 870,849 subscribers to whom it sent unsolicited direct marketing test messages or the 620,000 subscribers to whom its affiliate had sent unsolicited direct marketing e-mails.

Enforced remedial action required within 35 days:

1. Except in the circumstances referred to in paragraph (3) of Regulation 22 of PECR, neither transmit, nor instigate the transmission of unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient has previously notified VBL that they clearly and specially consent for the time being to such communications being sent by, or at the instigation of VBL.

Types of PECR breach

Breach of PECR Regulation 21: **4**

Breach of PECR Regulation 22: **4**

Breach of PECR Regulations 19 & 24: **3**

Breach of PECR Regulation 21 & 24: **1**



The Lead Experts Limited

10 October 2017

Monetary Penalty

PECR — Regulations 19 & 24

Between 4 May 2016 and 5 May 2016 The Lead Experts Limited (TLEL) instigated the transmission of 111,072 automated marketing calls to subscribers without their prior consent. Furthermore, contrary to Regulation 24 of PECR, TLEL did not identify the organisation (person) who was sending or instigating the automated marketing calls or provide the address of the organisation or a telephone number on which this organisation can be reached free of charge.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of communications comprising recorded matter for direct marketing purposes by means of an automated calling except:
 - a. Where the called line is that of a subscriber who has previously notified TLEL that for the time being they clearly and specifically consent to such communications being sent by, or at the instigation of, TLEL; and
 - b. Where the communication includes the name of TLEL and either the address of TLEL or a telephone number on which TLEL can be reached free of charge.

Hamilton Digital Solutions Limited

16 November 2017

Monetary Penalty

PECR — Regulation 22

Between 1 April 2016 and 19 September 2016, Hamilton Digital Solutions Limited (HDSL) used a public electronic telecommunications service for the purposes of instigating the transmission of 156,250 unsolicited communications by means of electronic mail to individual subscribers for direct marketing purposes contrary to Regulation 22 of PECR.

Enforced remedial action required within 35 days:

1. Except in the circumstances referred to in paragraph (3) of Regulation 22 of PECR, neither transmit, nor instigate the transmission of unsolicited communications for direct marketing purposes by electronic mail unless the recipient has previously notified HDSL that they consent for the time being to such communications being sent by, or at the instigation of HDSL.

21 December 2017

No Monetary Penalty

DPA— 6th Principle

On 28 July 2017, the data controller had a backlog of 919 subject access requests from individuals, some of which dated back to 2012. The data controller's recovery plan involved eliminating the backlog by October 2018 and from 31 January 2018 dealing with any new subject access requests from individuals without undue delay. On 10 November 2017, there were 793 cases over 40 days old.

The data controller failed to inform the individuals, whether their personal data is being processed by or on behalf of the data controller, without undue delay, and failed to communicate in an intelligible form information which may constitute personal data. Further, the data controller's internal systems, procedures and policies for dealing with subject access requests made under the DPA were unlikely to achieve compliance with the provisions of the DPA.

Enforced remedial action required within 10 months:

1. Inform the individuals whose access requests are over 40 days olds whether the personal data processed includes personal data of which those individuals (or any of them) are the data subjects and shall supply each of them with a copy of any such personal data so processed in accordance with the requirements of Section 7 of the DPA and the sixth data protection principle in that respect, subject only to the proper consideration and application of any exemption from, or modification to, Section 7 of the DPA provided for in or by virtue of part IV of the DPA which may apply.

Enforced remedial action required within 30 days:

1. Carry out changes to its internal systems, procedures and policies necessary to ensuring all subject access requests received by the data controller, in respect of the data controller, pursuant to Section 7 of the DPA are identified and complied with in accordance with the seven requirements of Section 7 of the DPA, and the sixth data protection principle in that respect, subject only to:
 - a. The proper consideration and application of any exemption from, or modification to, Section 7 of the DPA provided for in or by virtue of part IV of the DPA which may apply; and
 - b. The expectation that such requests are expressed with reasonable clarity and are properly addressed.
2. Continue to use his best endeavours to surpass the milestones outlined above.
3. Provide the Commissioner with a progress report at the beginning of each month, documenting in detail how the terms of this enforcement notice have been, or are being, implemented.



Attend our Data Protection Bootcamps

Join our Data Protection Bootcamps every month by WebEx or in person.

They provide:

- Accessible insights into the practicalities of operating in a GDPR-live environment
- Pragmatic recommendations on how to operationalise Data Protection law and reduce operational, legal and commercial risk
- Learning and networking opportunities with your peers

We also offer tailored in-house Data Protection training and awareness sessions.

For further information please contact us at DP_Bootcamps@uk.pwc.com



UK Monetary Penalty Notices (MPNs)

Require organisations to pay up to
£500,000 for serious breaches of the
Data Protection Act occurring on or
after 6 April 2010

<i>Total</i>	<i>54</i>
Private Sector	<i>48</i>
Public Sector	<i>6</i>
<i>Total Value</i>	<i>£4,207,500</i>

Royal & Sun Alliance Insurance plc (RSA)

5 January 2017

£150,000

DPA – 7th Principle

Factual background

Royal & Sun Alliance Insurance plc ('RSA') is a multinational general insurance company. It provides (among other things) personal insurance products and services to its customers.

At some point between 18 May 2015 and 30 July 2015, a portable 'Network Attached Storage' device (the 'device') was stolen by an unidentified member of staff or contractor from a server room in RSA's premises.

Access to the server room at RSA's premises requires use of an access card and key. 40 of RSA's staff and contractors (some of whom were non-essential) were permitted to access the DSR unaccompanied.

The device held, among other things, personal datasets containing:

- 59,592 customer names, addresses, bank account and sort code numbers; and
- 20,000 customer names, addresses and credit card 'Primary Account Numbers'.

The device did not contain expiry dates or CVV numbers. It was password protected but not encrypted. The device has not been discovered to date.

ICO finding

The ICO found that RSA did not have appropriate technical and organisational measures for ensuring so far as possible that such an incident would not occur (DPA – 7th Principle).

In particular:

- RSA did not encrypt the dataset prior to loading them on the device;
- RSA failed to physically secure the device in the server room;
- RSA failed to routinely monitor whether the device was online and (if not) raise alarm;
- RSA did not have CCTV installed inside the server room;
- RSA failed to restrict access to the server room to essential staff and contractors;
- RSA permitted staff and contractors to access the server room unaccompanied; and
- RSA failed to monitor access to the server room.

The ICO did not consider the contravention deliberate but held that RSA should have known or ought reasonably to have known that there was a risk that this contravention would occur. The ICO found that RSA had failed to take reasonable steps to prevent the contravention.

Harm

The ICO was satisfied that the contravention identified was 'serious' due to the number of affected individuals, the nature of the personal data that was held on the device and the potential consequences of the contravention.

The ICO held that the contravention was likely to cause substantial damage or substantial distress, taking into account:

- the nature of the personal data, in particular as it concerns financial information; and
- that portable devices have a high risk of loss or theft and require adequate security.

The ICO recognised that distress could be caused to RSA's customers if they knew their financial information might have been accessed by the individual who stole the device, further disseminated or misused. Financial damage could also arise from exposure to blagging and possible fraud.

Aggravating factors

- RSA was unable to pinpoint exactly when the device was stolen.
- RSA received 195 complaints about this incident.

Mitigating factors

- The device was password protected.
- The personal data held on the device was not easily accessible.
- So far as the Commissioner is aware, the information has not been further disseminated or accessed by third parties, and has not been used for fraudulent purposes.
- RSA notified its affected customers and offered free CIFAS protection for 2 years.
- RSA has now taken substantial remedial action.
- A monetary penalty may have a significant impact on the RSA's reputation and, to an extent, its resources.
- RSA has sought independent professional advice to assist with the remediation of this incident.
- There is no indication that any RSA customer has suffered a financial loss.

11 January 2017

£40,000

PECR – Regulation 21

Factual background

IT Protect Ltd's ('IT Protect') business involves making unsolicited marketing calls to elderly subscribers in order to sell a call blocking device to 'stop' unwanted marketing calls.

Between 6 April 2016 and 16 May 2016, IT protect made 157 unsolicited marketing calls to subscribers who were registered with the Telephone Preference Service ('TPS'). The TPS is a register of numbers allocated to subscribers who have notified the TPS that they do not wish to receive unsolicited calls for direct marketing purposes on those lines.

The ICO received 35 complaints about IT Protect from individual subscribers who were registered with the TPS. The TPS received 122 complaints about IT Protect and referred all of these to IT Protect and also notified the ICO. IT Protect did not respond to the TPS on 69 occasions.

IT Protect explained to the ICO that it had purchased opt-in data from a third party company, however it had not carried out any due diligence checks to ensure that they had given their consent to receive such calls from IT Protect.

ICO finding

The ICO found that IT Protect did not have the appropriate consent to make unsolicited direct marketing calls to subscribers registered with the TPS (Regulation 21 of PECR).

The ICO did not consider the contravention deliberate, but stated that IT Protect should have known or ought reasonably to have known that there was a risk that this contravention would occur. The ICO found that IT Protect had failed to take reasonable steps to prevent the contravention.

Harm

The ICO was satisfied that the contravention was 'serious' due to there being multiple breaches, the duration of the contravention and the number of complaints received.

Individual subscribers complained that the calls were misleading as they gave the impression that they were calling on behalf of BT and some complainants allege that IT Protect preyed on the elderly.

The contravention was exacerbated by the fact that IT Protect was making unsolicited marketing calls to elderly subscribers to sell them a call blocking device to 'stop' unwanted marketing calls.

Aggravating factors

- IT Protect may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.

Mitigating factors

- There is a potential for damage to IT Protect's reputation which may affect future business.

Total number of MPNs per year



2017: **54**

2016: **35**

2015: **18**

2014: **11**

2013: **18**

2012: **25**

18 January 2017

£50,000 – reduced on appeal to £20,000

PECR – Regulation 22

Factual background

LAD Media Limited ('LAD Media') is a lead generation and data brokerage business operating in the financial services, debt management and consumer claims sector.

Between 6 January 2016 and 10 March 2016 LAD Media instigated the sending of 393,872 direct marketing text messages to individuals. It had purchased the data used to send the messages from a third party data supplier and the text messages had then been sent on LAD Media's behalf by another third party. LAD Media provided examples of the opt-in statements which had been relied on to the ICO, which included (among others) the following:

'By agreeing to these terms and condition we may contact you about services or products offered by us or other companies in our group or approved by us, which we believe you may be interested in, or to carry out market research about our services or products or those of third parties. We may also pass information to other companies approved by us so that they may contact you about services or products, which they believe you may be interested in. Contact for these purposes may be by post, email, SMS or by other means as we may agree with you from time to time. This will override any registrations you may have with any preference services.'

During this period, 158 complaints were received by the GSMA's Spam Reporting Service or direct to the ICO, relating to the receipt of unsolicited direct marketing text messages sent on behalf of LAD Media. The GSMA's Spam Reporting Service allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA, who makes such complaints data available to the ICO.

ICO finding

The ICO found that LAD Media did not have the appropriate consent to send unsolicited direct marketing text messages to individuals (Regulation 22 of PECR).

The ICO did not consider the contravention deliberate but stated that LAD Media should have known or ought reasonably to have known that there was a risk that this contravention would occur.

The ICO found that LAD Media had failed to take reasonable steps to prevent the contravention, stating that it is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence.

Harm

The ICO was satisfied that the contravention was 'serious' due to the number of messages sent and number of complaints received.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Appeal

LAD Media appealed the ICO's MPN and the Tribunal substituted the ICO's MPN for an MPN on the same terms with the amount of the penalty amended to £20,000. The Tribunal found that there was a contravention of Regulation 22 of PECR as LAD Media did not have the necessary consents, the contravention was sufficiently serious and LAD Media knew or ought to have known the contravention would occur. However, the amount of the penalty was too high when considering the size of the company and the low levels of profit generated from the activity. Notably, the Tribunal set out some general factors which may be used to determine the amount of a monetary penalty:

- The circumstances of the contravention;
- The seriousness of that contravention, as assessed by the harm, either caused or likely to be caused, as a result; whether the contravention was deliberate or negligent; and the culpability of the person or organisation concerned, including an assessment of any steps taken to avoid the contravention.
- Whether the recipient of the MPN is an individual or an organisation, including its size and sector;
- The financial circumstances of the recipient of the MPN, including the impact of any monetary penalty;
- Any steps taken to avoid further contravention(s); and
- Any redress offered to those affected.

The Data Supply Company Limited

27 January 2017

£20,000

DPA – 1st Principle

Factual background

The Data Supply Company is a list or data broker which obtains personal data from various sources and sells this information as marketing leads to organisations for the purpose of sending direct marketing to those individuals.

Between 19 June 2015 and 21 September 2015, 174 complaints were received by the GSMA's Spam Reporting Service or direct to the ICO, relating to the receipt of 21,045 unsolicited direct marketing text messages about pay day loans. The GSMA's Spam Reporting Service allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA, who makes such complaints data available to the ICO. The ICO established that the person responsible for sending those text messages had obtained the data from The Data Supply Company. The Data Supply Company had provided 580,302 records containing personal data.

ICO finding

The ICO found that The Data Supply Company did not process the personal data it obtained from individuals fairly and lawfully (DPA – 1st Principle).

In particular:

- The relevant individuals were not informed that their personal data would be disclosed to The Data Supply Company, or the organisations to which The Data Supply Company sold the data on to, for the purpose of sending direct marketing text messages.
- The disclosures given would not be within those individuals' reasonable expectations.

The ICO did not consider the contravention deliberate but The Data Supply Company should have known or ought reasonably to have known that there was a risk that this contravention would occur and that they would be of a kind likely to cause substantial damage or substantial distress.

The ICO found that The Data Supply Company had failed to take reasonable steps to prevent the contravention, stating that it had failed to undertake proper due diligence when both buying and selling personal data to ensure that the processing was fair.

Harm

The ICO was satisfied that the contravention was 'serious' due to the number of records containing personal data being disclosed without the data subjects' knowledge or consent.

The ICO found that the contravention was of a kind likely to cause substantial distress.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- The Data Supply Company has informed the ICO that it is no longer trading in personal data.

23 February 2017

£200,000

DPA – 7th and 8th Principles

Factual background

HCA International Ltd ('HCA') owns private hospitals including the Lister Hospital in London. It provides a wide range of services to private patients, including IVF treatment.

Beginning in 2009, Lister Hospital sent unencrypted audio recordings of private consultations by email to a data processor in India for transcription. HCA was aware that the data processor used an unsecured FTP server to store the recordings. The server did not have an authentication process to restrict access to the transcripts.

On 8 April 2015, a patient informed the hospital that transcripts of consultations containing confidential and sensitive personal data could be accessed via an internet search engine.

ICO finding

The ICO found that HCA failed to take appropriate technical measures against unauthorised or unlawful processing of personal data in contravention of the seventh data protection principle. In particular:

- HCA sent unencrypted recordings by email to the data processor in India;
- HCA had no guarantee that the data processor would use a secure FTP server to store the recordings and then send completed transcripts to the hospital;
- HCA had no guarantee that the data processor would erase the recordings after they had been transcribed;
- HCA failed to monitor the data processor in relation to any security measures taken by it; and
- HCA did not have a DPA compliant contract with the data processor in relation to the processing.

The contravention was ongoing from 2009 until HCA took remedial action following the security breach on 8 April 2015.

The ICO did not consider the contravention deliberate but HCA should have known or ought reasonably to have known that there was a risk that this contravention would occur and that it would be of a kind likely to cause substantial distress. The ICO found that HCA failed to take reasonable steps to prevent the contravention.

The ICO also found that the eighth data protection principle was contravened by HCA, in that data was transferred outside the EEA without an adequate level of protection.

Harm

The ICO was satisfied that the contravention was serious as the transcripts contained confidential and sensitive personal data. The ICO also had regard to the number of affected individuals and the possible consequences.

The ICO considered that the contravention would cause distress to patients and that such distress was likely to be substantial, having regard to the number of affected individuals and the nature of the personal data involved.

Aggravating factors

- No mention of aggravating factors.

Mitigating factors

- HCA voluntarily reported the breach to the ICO
- HCA were fully co-operative with the ICO
- HCA have taken substantial remedial action
- There will be a significant impact on HCA's reputation as a result of this security breach

19

Increase of total MPNs
in 2017 verses 2016

17

Increase of total MPNs
in 2016 verses 2015



3 March 2017

£270,000

PECR – Regulations 19 & 24

Factual background

Media Tactics generates leads in relation to individuals making a claim for a PPI refund.

Between 24 July 2014 and 9 June 2015 the ICO received 182 complaints about the receipt of unsolicited automated marketing calls made from telephone numbers used by Media Tactics. On further investigation, it was found that between 13 November 2014 and 9 June 2015 Media Tactics made 22,065,627 automated direct marketing calls.

On 24 August 2015 the ICO wrote to Media Tactics informing it that the ICO had evidence that it had made over 22 million automated direct marketing calls, that the ICO had received 182 complaints and asked Media Tactics to provide evidence that the recipients of the calls had consented to receiving automated marketing calls from Media Tactics.

Media Tactics informed the ICO that it purchased data from a number of different third party data providers, who had given warranties that the data was 'opted-in', and that the data had been screened against the Telephone Preference System. Most of the websites from which the telephone numbers of the complainants had originally been sourced belonged to payday loan and insurance brokers.

Many of the privacy notices on the identified websites were generic and unspecific and did not refer to the data being used for the purposes of making automated direct marketing calls. Only one of the privacy notices identified Media Tactics as a recipient of the data, but this was in a list of over 200 organisations.

ICO finding

The ICO found that Media Tactics instigated over 22 million automated direct marketing calls without prior consent of the individuals called (Regulation 19 of PECR).

In particular, the ICO found that between 13 November 2014 and 9 June 2015 Media Tactics instigated the transmission of 22,065,627 automated marketing calls to subscribers without their prior consent. It also found that Media Tactics did not identify the person who was sending or instigating the automated marketing calls and provide the address of the person or a telephone number on which this person could be reached free of charge.

The ICO did not consider the contravention deliberate but Media Tactics should have known or ought reasonably to have known that there was a risk that this contravention would occur. Further, the ICO found that Media Tactics had failed to undertake adequate due diligence on its data providers.

Harm

The ICO was satisfied that the contravention was 'serious' because Media Tactics instigated the making of over 22 million automated marketing calls to subscribers without their prior consent, which resulted in 182 complaints being made to the Commissioner.

The Commissioner was also satisfied that contravention was of a kind likely to cause substantial distress and Media Tactics ought to have known that it was only a matter of time before substantial distress to the recipients of the calls was likely to be caused. The ICO indicated that the failure to identify Media Tactics as the caller or provide an address or telephone number on which it could be contacted free of charge was a factor likely to cause substantial damage or distress.

Aggravating factors

- The director of Media Tactics had been involved in the lead generation business for several years and had a history of contact with the ICO. Media Tactics should therefore have had a good level of awareness of PECR and its requirements.

Mitigating factors

- There is a potential for damage to Media Tactics's reputation which may affect future business.

Munee Hut LLP

10 March 2017

£20,000

PECR – Regulation 22

Factual background

Munee Hut LLP ('Munee Hut') is a credit lending and brokerage business which markets its services through affiliates which send marketing text messages directing recipients to its website. Between 1 May 2015 and 22 March 2016, approximately 64,000 unsolicited direct marketing text messages were sent on the company's behalf by its affiliate, a company based in Belize. During this period, 885 complaints were made to GSMA's Spam Reporting Service. The GSMA's Spam Reporting Service allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA, who makes such complaints data available to the ICO.

The data had been obtained from a number of different websites (loan companies and a prize draw website) which had generic and unspecific privacy notices which did not indicate that the data would be used for sending direct marketing text messages by or on behalf of the company.

ICO finding

The ICO found that between 1 May 2015 and 22 March 2016, Munee Hut instigated the transmission of approximately 64,000 unsolicited direct marketing messages to individual subscribers without the requisite consent (Regulation 22 of PECR).

As the instigator of the text messages, it was the responsibility of the company to ensure that sufficient consent had been acquired. The ICO was satisfied that the company did not have the consent of the subscribers.

The ICO stressed that it was not acceptable to rely on assurances of indirect consent without undertaking proper due diligence. It found that a reputable list broker should provide full details of individual's consent to be contacted. If a broker could not provide such information, the buyer should not use the list. Munee Hut relied on contractual assurances, but did not carry out a proper review of the privacy notices of the websites of which the data had been obtained.

The ICO did not consider the contravention deliberate, but Munee Hut should have known or ought reasonably to have known that there was a risk that these contraventions would occur.

Harm

The ICO was satisfied that the contravention was 'serious' due to the fact that 64,000 messages were sent and 885 complaints received.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Data breach by a barrister (redacted)

10 March 2017

£1,000

DPA – 7th Principle

Factual background

The data controller is a senior barrister who specialises in family law.

The barrister created documents at home on her standalone desktop computer. The computer was password protected but the files were unencrypted. In January 2013, the Bar Council issued guidance to barristers that specific files may require encryption to prevent unauthorised access to confidential matters by shared users. On 19 September 2015, the barrister's husband temporarily uploaded the barrister's files (725 documents) to an online directory to back them up before a software update.

On 5 January 2016, a local authority solicitor informed the barrister's Chambers that the documents containing confidential and sensitive information could be accessed on the internet. 15 of these were cached and indexed so could be easily accessed using a recognisable word. 6 of the 15 contained confidential and highly sensitive information relating to lay clients who were involved in proceedings in the Court of Protection and the Family Court.

Between 200 and 250 individuals were affected by this incident, including vulnerable adults and children.

ICO finding

The ICO found that the barrister did not have in place appropriate technical measures for ensuring that such an incident would not occur, i.e. for ensuring that her files could not be accessed by unauthorised third parties (DPA – 7th Principle). In particular, the barrister did not encrypt her files.

The Commissioner considered the contravention the result of a serious oversight rather than deliberate intent to ignore or bypass the provisions of the DPA. However, the Commissioner was satisfied that the barrister ought reasonably to have known that there was a risk that such an incident would occur unless she ensured that the files held on her desktop computer were technically secured.

Harm

The ICO was satisfied that the contravention was 'serious' due to the number of affected individuals, the nature of the personal data contained in the files and the potential consequences.

The files contained confidential and highly sensitive information relating to 200 to 250 individuals, some of whom were adults and children in vulnerable circumstances. The ICO considered that the contravention was of a kind likely to cause distress to the barrister's lay clients if they knew that their confidential and highly sensitive information has been accessed by unauthorised third parties and could be further disseminated or misused.

15 March 2017

£60,000

DPA – 7th Principle

Factual background

On 14 April 2014, a third party collected some redundant furniture from the Council as part of an office move. The furniture included a number of filing cabinets used by the children's social work team.

On 18 April 2014, a member of the public bought one of the filing cabinets from a second hand furniture shop. The filing cabinet was delivered to their home address and was found to contain case files, including sensitive information relating to (among others) seven children.

The Council did not keep a record of how many pieces of furniture were collected by the third party and it was not clear which team was responsible for ensuring that the furniture was empty prior to disposal.

ICO finding

The ICO found that the Council did not have in place appropriate organisational measures for ensuring that such an incident would not occur, i.e. for ensuring that the office furniture was empty prior to disposal (DPA – 7th Principle).

In particular, the Council did not have adequate written procedure governing how office furniture disposal should be managed.

The ICO did not consider the contravention deliberate, however, the Council ought reasonably to have known that there was a risk that this contravention would occur unless it ensured the office furniture disposal process was governed by an adequate written procedure.

Harm

The ICO was satisfied that the contravention was 'serious' due to the highly sensitive nature of some of the personal data that was left in the furniture and the potential consequences.

The ICO also considered that the contravention was of a kind likely to cause distress to the affected individuals because the personal data could be further disseminated or misused and that the damage or distress was likely to be substantial having regard to the number of affected individuals and the highly sensitive nature of some of the personal data held in the files.

Aggravating factors

- Some of the office furniture is still unaccounted for.

Mitigating factors

- The information in the filing cabinet was recovered from the member of the public after eight days, as soon as the Council was notified.
- The Council has taken remedial action.
- The Council referred this incident to the ICO and was co-operative during the investigation.
- A monetary penalty may have a significant impact on the Council's reputation and (to some extent) its resources.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- The barrister was fully co-operative with the ICO.
- The barrister has taken remedial action.

Total value of MPNs per year



2017: **£4,207,500**

2016: **£3,245,500**

2015: **£2,031,250**

2014: **£1,152,500**

2013: **£1,520,000**

2012: **£2,430,000**

Honda Motor Europe Limited t/a Honda (U.K.)

20 March 2017

£13,000

PECR – Regulation 22

Factual background

Honda Motor Europe Limited ('Honda') is responsible for the sale of Honda products in the UK, including cars and motorbikes. It also coordinates Honda's operations in Europe.

Between 1 May 2016 and 22 August 2016 Honda sent a large number of e-mails to individuals entitled 'would you like to hear from Honda?' in order to clarify marketing preferences. The e-mail was sent to those individuals on the database where no 'opt in' or 'opt out' information was held.

Honda explained to the ICO that it had sent the e-mail as a service email, rather than as a marketing e-mail.

Honda obtains personal data of individuals and their specific preferences for direct marketing purposes in a number of ways, including through authorised dealers who are expected to adhere to Honda's Data Management Policy and Guidelines. Due to a design flaw, some dealers had input data onto Honda's central customer database and had confirmed that an individual had agreed to direct marketing but had failed to complete the actual marketing preferences field as a yes/no completion of the field was not mandatory.

ICO finding

The ICO found that between 1 May 2016 and 22 August 2016, Honda instigated the transmission of 289,093 unsolicited communications by e-mail to individual subscribers for the purposes of direct marketing without consent (Regulation 22 of PECR).

As the instigator of the e-mails, Honda was responsible for ensuring that sufficient consent had been acquired. The ICO was satisfied that Honda did not have the requisite consent.

The ICO also found Honda had failed to take reasonable steps to prevent the contraventions.

The Commissioner did not consider the contravention deliberate, however, Honda knew or ought to reasonably have known that there was a risk that these contraventions would occur.

Harm

The Commissioner was satisfied that the contravention was 'serious' because of the number of individuals affected.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Flybe Limited

20 March 2017

£70,000

PECR – Regulation 22

Factual background

Flybe Limited ('Flybe') is a large regional airline carrier, based in Exeter.

On 15 August 2016 it sent 3,662,973 e-mails to individuals entitled 'Are your details correct?'. 3,333,940 of these were successfully received. The e-mail advised individuals to amend any out of date information and update any marketing preferences. The e-mail also instructed that by updating their preferences they may be entered into a prize draw.

Flybe used a third party agent to distribute bulk e-mails. The agent holds Flybe's customer database and maintains the list of opt-in and opt-out individuals for direct marketing purposes. On this occasion, Flybe requested that its agent send e-mails to customers who had previously explicitly opted out of direct marketing.

ICO finding

The ICO found that on 15 August 2016, Flybe instigated the transmission of 3,333,940 unsolicited communications by e-mail to individual subscribers for the purposes of direct marketing without their consent (Regulation 22 of PECR).

In addition, Flybe also instigated the sending of a further 329,033 marketing e-mails. Although these were not received by individuals it evidences an attempt to send large volumes of marketing e-mails to individuals without consent to do so.

As the instigator of the e-mails, it was the responsibility of Flybe to ensure that sufficient consent had been acquired. The ICO was satisfied that Flybe did not have the required consent and deliberately contravened Regulation 22 of PECR.

Harm

The ICO was satisfied that the contravention was 'serious' due to the large volume of direct marketing emails sent to subscribers without their consent. Flybe were aware that the email was being sent to individuals who according to its records, had previously indicated that they did not consent to receive direct marketing.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

PRS Media Limited (trading as Purus Digital)

27 March 2017

£140,000

PECR – Regulation 22

Factual background

PRS Media Limited ('PRS') is an advertising marketing company. It markets services using different forms of media, including email and text message, directing recipients to websites.

Between 1 January 2016 and 17 May 2016, the GSMA's Spam Reporting Service had received 2,628 complaints about the receipt of unsolicited direct marketing text messages sent on behalf of PRS. The GSMA's Spam Reporting Service allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA, who makes such complaints data available to the ICO.

Following the receipt of an Information Notice from the ICO, PRS explained that it had sourced the personal data for the text messaging from a competition and a prize draw website it owned. A condition of the entry to the competitions included a compulsory agreement to marketing at the point of sign-up. Although reference was made to this in both its terms and conditions and privacy policy, both were generic and unspecific. At no point was an individual able to express a preference on how they may be contacted.

ICO finding

The ICO found that PRS did not have the consent of the 4,357,453 subscribers to whom it sent unsolicited direct marketing text messages (PECR – Regulation 22).

Harm

The ICO was satisfied that the contravention was serious due to the number of direct marketing text messages that were sent to subscribers without their consent, and the number of subsequent complaints made.

Aggravating factors

- PRS had failed on two separate occasions to answer requests for information from the ICO and it required the service of an Information Notice to compel a response.
- The response received from PRS to the Information Notice provided unsatisfactory answers to the questions asked and figures provided were at odds with the Commissioners own findings.
- PRS did not identify the person who was sending or instigating direct marketing text messages.

Mitigating factors

- There were no mitigating features.

Xternal Property Renovations Ltd

28 March 2017

£80,000

PECR – Regulation 21

Factual background

Xternal Property Renovations Ltd (the 'Company') provides property maintenance and repair services to members of the public. The Commissioner wrote to the Company on 10 December 2015 regarding its compliance with PECR following a number of complaints having been made by subscribers registered with the Telephone Preference Service ('TPS') about unsolicited direct marketing telephone calls.

In February 2016 the Company responded, explaining that it had endeavoured to acquire legitimate and authorised third party customer information. However, the Company did not provide the identity of the company or companies from whom the data had been acquired, nor any evidence of the due diligence performed on the list provider or the data itself. It also became apparent that the Company had not performed any TPS screening as it was still in the process of completing the application process for its licence.

Between 14 August 2015 and 11 April 2016, the ICO received 131 complaints about unsolicited direct marketing calls made by the Company. Of those complaints, 94 were made to the TPS, with a further 37 made direct to the ICO. All of these complaints were made by individual subscribers who were registered with the TPS.

ICO finding

The ICO found that the Company made a number of unsolicited calls for direct marketing purposes without the appropriate consent (Regulation 21 of PECR).

Between 14 August 2015 and 11 April 2016, the Company used a public telecommunications service to make 131 unsolicited direct marketing calls. The called lines were numbers listed on the register of numbers kept by the Commissioner in accordance with Regulation 26, contrary to Regulation 21(1)(b) of PECR.

The Commissioner was also satisfied for the purposes of Regulation 21 that the 131 complaints were made by subscribers who had registered with the TPS at least 28 days prior to receiving the calls and they had not given their prior consent to the Company to receive calls.

The Commissioner considered that in this case the Company did not deliberately contravene Regulation 21 of PECR, however, the Company ought reasonably to have known the risk of contravening PECR because the Company knew people were complaining about calls received. The Commissioner also found that the Company failed to take reasonable steps to prevent the contraventions.

3 April 2017

£9,000

DPA – 1st Principle, 2nd Principle

Factual background

WWF-UK is an international non-governmental organization founded in 1961, working in the field of wilderness preservation, and the reduction of human impact on the environment.

Sharing personal data with third parties

WWF-UK was a member of a Reciprocate Scheme, which was run by an external company and enabled participating charities to share or swap the personal data of donors or prospective donors. Between 2012 and 2015 WWF-UK provided quarterly updates to the Reciprocate Scheme and in total shared 174,512 donor records, including details such as the name and addresses of donors.

WWF-UK's privacy notice stated that 'from time to time we may agree with carefully selected organisations to swap data, so that we can write to each other's supporters. If you do not wish us to share your data in this way, please tick this box...'

Wealth screening

WWF-UK used the services of a wealth screening company to analyse the financial status of its supporters in order to identify those that would have the capacity and propensity to make a larger donation to charity. The personal data which WWF-UK provided to the wealth screening company included supporters' names and addresses and information relating to their donation history.

WWF-UK confirmed that it had undertaken such activity on three occasions: in 2006, 2011, and 2016. It wealth-screened 211,352 records in 2011, and a further 580,098 records in 2016. These figures do not necessarily reflect the number of individuals whose data was screened, as some supporters' data may have been screened more than once. The total number of individuals whose personal data was processed for the purposes of wealth analysis was 643,531.

Tele-matching

WWF-UK began tele-matching (using personal data to obtain and use telephone numbers which data subjects have chosen not to provide) in 2006 and stopped in March 2016. From 6 April 2010 until March 2016 it tele-matched a total of 83,475 records relating to 55,684 supporters.

ICO finding

The Commissioner was satisfied that these contraventions were deliberate, in the sense that the actions of WWF-UK were deliberate. While WWF-UK may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so.

Alternatively, WWF-UK ought reasonably to have known that there was a risk that the contraventions would occur, and that they would be of a kind likely to cause substantial damage or distress.

Harm

The Commissioner did not comment on the harm associated with the contravention in this case. However, the complaints received indicate that at least some of the affected individuals suffered some distress from receiving these calls.

In particular:

- 'I get these calls from early morning to late at night, I'm disabled and I worry about these calls.'
- 'I was concerned about how this company had obtained my details – particularly my name. My number is TPS-registered and has been ex-directory for more than 30 years.'
- 'I object to being called an idiot and told 'it'll serve you right when you can't pay your bills'. Nasty and could really upset an older person.'

Aggravating factors

- Between 7 September 2015 and 30 November 2015, 109,726 direct marketing calls were made by the Company to individual subscribers registered with the TPS. This represented 81% of the total calls made by the Company in the same period.
- As late as February 2016 the Company had not performed any TPS screening as it had not yet completed its TPS annual licence application process.
- The Company did not identify the person instigating the calls and deliberately misled subscribers by using generic company names which had no relation to the Company.
- There was a failure to fully cooperate with the Commissioner.
- The Company is a private organisation within a competitive direct marketing industry where continuous breaches of PECR could create an unfair advantage.

Mitigating factors

- There is a potential for damage to the Company's reputation which may affect future business.

Sharing personal data with third parties

The ICO found that WWF-UK unfairly processed individuals' personal data because the terms of its privacy notice were unduly vague and/or ambiguous and did not provide data subjects with adequate information as to how their personal data would be shared via the schemes (DPA – 1st Principle). The ICO also found that the sharing of personal data via the schemes was incompatible with the purposes explained in WWF-UK's privacy notices (DPA – 2nd Principle).

Wealth screening

The ICO found that the WWF-UK unfairly processed individuals' personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that WWF-UK would adopt these techniques (through the WWF-UK's privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

Tele-matching

The ICO found that it was unfair for the WWF-UK to use the data for data-matching and/or tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

Harm

The ICO considered that the contraventions were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from the WWF-UK; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- WWF-UK had followed the unlawful practices described over a period of several years and on a continuing basis.
- WWF-UK's practices appear to have been driven at least in part by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- WWF-UK had contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the DPA and Directive 95/46/EC.
- By failing to adequately explain to data subjects how their personal data would be used, WWF-UK has deprived them of control and informed decision-making about their personal data to a significant extent.
- WWF-UK's activities as described have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to unsolicited direct marketing communications. It is likely that many individuals will have been persuaded by WWF-UK to increase their financial support. Those financial consequences will to a significant extent have flowed from WWF-UK's unlawful data protection practices.

Mitigating factors

- WWF-UK co-operated with the Commissioner's investigations.
- WWF-UK is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- WWF-UK has taken remedial action.
- WWF-UK's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

The increase of total value of MPNs

2017: **£962,000**

2016: **£1,214,250**

2015: **£878,750**



3 April 2017

£12,000

DPA – 1st Principle, 2nd Principle

Factual background

Wealth screening

The Royal British Legion ('RBL') used the services of a wealth screening company to analyse the financial status of its supporters in order to identify those that would have the capacity and propensity to make a larger donation to charity. The personal data which RBL provided to the wealth screening company included supporters' names and addresses and information relating to their donation history. 2,445,670 records were scanned in 2014.

Data-matching and tele-matching

RBL also used the services of external companies to undertake data-matching and tele-matching on its behalf since 2010. Data-matching is the use of personal data to obtain and use other items of personal data which data subjects may have chosen not to provide to the data controller, and tele-matching is data-matching with telephone numbers. RBL estimated that it is likely to have tele-matched approximately 900,000 records and data-matched 52,966 email addresses to the personal data of supporters since 2010.

ICO finding

The ICO was satisfied that these contraventions were deliberate, in the sense that the actions of RBL were deliberate. While RBL may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so.

Alternatively, RBL ought reasonably to have known that there was a risk that the contraventions would occur, and that they would be of a kind likely to cause substantial damage or distress.

Wealth screening

The ICO found that the wording of RBL's privacy notices in place at the relevant time did not indicate that personal data may be processed for the purpose of wealth analysis, nor had sufficient information been provided to supporters to enable them to understand what would be done with their personal data in terms of screening and object to such processing if they so wished (DPA – 1st Principle). In addition, the processing of personal data for the purposes of wealth analysis was incompatible with the purpose for which the data were obtained (DPA – 2nd Principle).

Data-matching and tele-matching

The ICO also found that RBL did not have the consent of the data subjects to use individuals' personal data to undertake data-matching and/or tele-matching and that such activities were neither compatible with the purposes explained in RBL's privacy notices nor in the reasonable expectation of the individuals affected (DPA – 1st and 2nd Principles).

Harm

The ICO considered that the contraventions were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways (where data-matching and wealth screening took place).

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from the RBL; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- RBL has followed the unlawful practices described over a period of several years.
- RBL's practices appear to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- RBL has contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the Data Protection Act 1998 and Directive 95/46/EC.
- By failing to adequately explain to data subjects how their personal data would be used, RBL has deprived them of control and informed decision-making about their personal data to a significant extent.
- RBL's activities as described have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to increased direct marketing communications from RBL. It is likely that many individuals will have been persuaded by RBL to increase their financial support. Those financial consequences will to a significant extent have flowed from RBL's unlawful data protection practices.

Mitigating factors

- RBL co-operated with the Commissioner's investigations.
- RBL is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- RBL has taken remedial action.
- RBL's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

3 April 2017

£18,000

DPA – 1st Principle, 2nd Principle

(PECR – Regulation 22 also considered, but was not a basis for the monetary penalty)

Factual background

The International Fund for Animal Welfare (‘IFAW’) is one of the largest animal welfare and conservation charities in the world.

Sharing personal data with third parties

The IFAW shared personal data as part of a Reciprocate Scheme. The Reciprocate Scheme was run by an external company and enabled participating charities to share or swap the personal data of donors or prospective donors. The IFAW participated in the Reciprocate Scheme and another similar scheme between 2011 and September 2015 inclusive. During this period, 4,948,633 records were disclosed, some of which may have been shared more than once.

Wealth screening

The IFAW also provided personal data to wealth screening companies. The personal data which IFAW provided to the wealth screening companies included supporters’ names and addresses, as well as internal coding information related to the donation history of the relevant data subject. The IFAW submitted a total of 685,956 records for wealth screening in 2012 and 2013, relating to 466,206 individual supporters.

Data-matching and tele-matching

The IFAW also used the services of an external company to undertake tele-matching on its behalf since at least 1995. Data-matching is the use of personal data to obtain and use other items of personal data which data subjects may have chosen not to provide to the data controller, and tele-marketing is a data-matching by which telephone numbers are obtained and used. The IFAW matched 220,286 telephone numbers to supporters for whom it had other personal data between 2006 and 2016. IFAW also used the services of an external company to match e-mail addresses to individual supporter records in 2012 and 2013. The IFAW matched 50,282 email addresses to the personal data of supporters, and proceeded to email all of them.

ICO finding

The ICO was satisfied that the contraventions of the Data Protection Act 1998 (‘DPA’) were deliberate, in the sense that the actions of the IFAW were deliberate. While the IFAW may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. The ICO also found that the IFAW failed to take reasonable steps to prevent the contraventions of the DPA from occurring.

Sharing personal data with third parties

The ICO found that IFAW unfairly processed individuals’ personal data because the terms of its privacy notice were unduly vague and/or ambiguous and did not provide data subjects with adequate information as to how their personal data would be shared via the schemes (DPA – 1st Principle). The ICO also found that the sharing of personal data via the schemes was incompatible with the purposes explained in IFAW’s privacy notices (DPA – 2nd Principle).

Wealth screening

The ICO found that the IFAW unfairly processed individuals’ personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that IFAW would adopt these techniques (through the IFAW’s privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

Data-matching and tele-marketing

The ICO found that it was unfair for the IFAW to use the data for data-matching and/or tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

The ICO also considered that by sending emails to persons who had not provided their specific consent to receiving direct marketing e-mails from IFAW, IFAW contravened Regulation 22 of PECR. This contravention was recorded by the ICO as an additional matter of concern but was not used as a basis for the MPN.

Harm

The ICO considered that the contraventions of the DPA were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from the IFAW; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

3 April 2017

£15,000

DPA – 1st Principle, 2nd Principle

(PECR – Regulation 21 also considered, but was not a basis for the monetary penalty)

Factual background

The Guide Dogs for the Blind Association ('GDBA') is a British charitable organisation founded in 1934.

Wealth screening

The GDBA used the services of wealth screening companies to analyse the financial status of its supporters in order to identify wealthy or high value individuals. The personal data which the GDBA provided to the wealth screening companies included supporters' names and addresses and information relating to their donation history. The GDBA informed the ICO that it had undertaken such activity in respect of its entire database of donors in 2008 and 2012, and more specific activity in 2010 and 2015. In total, the GDBA performed wealth screening on over 1.7m data subjects.

Data-matching and tele-matching

The GDBA had used the services of an external company to undertake tele-matching on its behalf since at least 2010. The GDBA has 248,094 matched telephone numbers on its database, of which 165,730 are Telephone Preference Service ('TPS') registered. The TPS is a register of numbers allocated to subscribers who have notified the TPS that they do not wish to receive unsolicited calls for direct marketing purposes on those lines. 163,180 of those have been added to the database since 6 April 2010.

The GDBA did not have specific consent from data subjects for whom it had matched telephone numbers, but who were TPS registered, to receive live telephone calls from the GDBA. It relied on generic consents provided to it by its commercial third party tele-matching data provider. Those generic consents referred only to contact from third parties and not to the GDBA. The GDBA accepted that until the summer of 2015, it did not screen its tele-matched calls against the TPS registration list.

The GDBA also used the services of an external company to identify donors to the GDBA who had not agreed to gift aid their donations by reference to donations they had made to other charitable organisations where gift aid was agreed. Those identified donors would then be contacted by the GDBA with material about using gift aid.

ICO finding

The ICO was satisfied that the contraventions of the Data Protection Act 1998 ('DPA') were deliberate, in the sense that the actions of the GDBA were deliberate. While the GDBA may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. The ICO also found that the GDBA failed to take reasonable steps to prevent the contraventions of the DPA from occurring.

Aggravating factors

- IFAW had followed the unlawful practices described above over a period of several years.
- IFAW's practices appear to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- IFAW had contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the DPA and Directive 95/46/EC.
- The number of affected persons by the various breaches of the DPA is considerably higher than those which specifically form the contraventions in this Notice because of the time period when some of the contraventions of the DPA occurred (i.e. prior to the power to impose a monetary penalty).
- By failing to adequately explain to data subjects how their personal data would be used, IFAW has deprived them of control and informed decision-making about their personal data to a significant extent.
- IFAW's activities have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to increased direct marketing communications from IFAW and/or other charities. It is likely that many individuals will have been persuaded – by IFAW and/or other charities – to increase their financial support. Those financial consequences will to a significant extent have flowed from IFAW's unlawful data protection practices.
- It is likely that IFAW has also contravened Regulation 22 of PECR.

Mitigating factors

- IFAW co-operated with the Commissioner's investigations.
- IFAW is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- IFAW has taken remedial action.
- IFAW's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.
- Company ought reasonably to have known the risk of contravening PECR because the Company knew people were complaining about calls received. The Commissioner also found that the Company failed to take reasonable steps to prevent the contraventions.

Wealth screening

The ICO found that the GDBA unfairly processed individuals' personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that GDBA would adopt these techniques (through the GDBA's privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

Data-matching and tele-matching

The ICO also found that it was unfair for the GDBA to use the data for data-matching and/or tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

The ICO also considered that by making telephonic contacts with persons who had not provided their specific consent to receiving direct marketing telephone calls from the GDBA and who were TPS registered the GDBA had contravened Regulation 21 of PECR. This contravention was recorded by the ICO as an additional matter of concern but was not used as a basis for the MPN.

Harm

The ICO considered that the contraventions of the DPA were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from the GDBA; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- The GDBA had followed the unlawful practices described above over a period of several years.
- The GDBA's practices appear to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- The GDBA had contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the DPA and Directive 95/46/EC.
- By failing to adequately explain to data subjects how their personal data would be used, the GDBA had deprived them of control and informed decision-making about their personal data to a significant extent.
- The GDBA's activities as described above have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to increased direct marketing communications from the GDBA. It is likely that many individuals will have been persuaded by the GDBA to increase their financial support. Those financial consequences will to a significant extent have flowed from the GDBA's unlawful data protection practices.
- It is likely that the GDBA have also contravened Regulation 21 of PECR.

Mitigating factors

- The GDBA co-operated with the Commissioner's investigations.
- The GDBA is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- The GDBA has taken remedial action.
- The GDBA's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.
- Would be of a kind likely to cause substantial damage or distress.



Sector

	Public	Private
2017:	6	48
2016:	6	29
2015:	3	15

3 April 2017**£6,000****DPA – 1st Principle, 2nd Principle**

(PECR – Regulation 22 also considered, but was not a basis for the monetary penalty)

Factual background

Oxfam is an international confederation of charitable organisations focused on the alleviation of global poverty.

Tele-matching

During the period 2003 until August 2015, Oxfam used the services of external companies to undertake tele-matching on its behalf. Tele-matching is data-matching by which telephone numbers which data subjects may have chosen not to provide are obtained and used.

Since 2011, Oxfam tele-matched a total of 267,521 records of donors. Oxfam used the telephone numbers obtained through tele-matching to make live marketing calls. Oxfam did not inform individuals that their data would be processed in this way.

Text message donation campaigns

Between August 2013 and July 2015, Oxfam undertook two campaigns that allowed individuals to donate to Oxfam via SMS text. Individuals who donated to the campaign received a bounce back text message and were automatically opted-in to receive further text and telephone marketing. In addition, 40,504 individuals received between one to four further marketing text messages as part of further campaigns in the following 13 months.

ICO finding**Tele-matching**

The ICO found that it was unfair for Oxfam to use the data for tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

The ICO was satisfied that the contravention of the Data Protection Act 1998 ('DPA') was deliberate, in the sense that the actions of Oxfam were deliberate. While Oxfam may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. The ICO also found that Oxfam failed to take reasonable steps to prevent the contraventions of the DPA from occurring.

Text message donation campaigns

The ICO considers that bounce back text messages as part of two separate Oxfam campaigns were sent for the purposes of direct marketing since they informed supporters of Oxfam's intention to make further marketing approaches in the future. The Commissioner also found that Oxfam did not have the requisite consent to send direct marketing text messages to individuals who made donations via SMS text messages. This was considered to be a likely contravention of Regulation 22 of PECR. This contravention was recorded by the ICO as an additional matter of concern but was not used as a basis for the MPN.

Harm

The ICO considered that the contravention of the DPA was serious because of the length of time over which the contravention took place, the number of data subjects whose rights were infringed

and the data subjects were likely to have been affected by this contravention in significant practical ways.

The ICO was satisfied that the contravention was of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from Oxfam; and
- given the scale and duration of the contravention, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- Oxfam has followed the unlawful practice described above over a period of several years and on a continuing basis.
- Oxfam's practice appear to have been driven at least in part by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- Oxfam has contravened the fundamental rights of very large numbers of individuals not to be subject to unlawful direct telephone marketing and to have their personal data processed in accordance with the DPA and Directive 95/46/EC.
- Oxfam's activities as described above have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to unsolicited direct marketing communications. It is likely that many individuals will have been persuaded by Oxfam to increase their financial support. Those financial consequences will to a significant extent have flowed from Oxfam's unlawful practice described above.
- It is likely that Oxfam has also contravened Regulation 22 of PECR.

Mitigating factors

- Oxfam co-operated with the Commissioner's investigations.
- Oxfam is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- Oxfam has changed its television advertisements in light of the Commissioner's investigation.
- Oxfam's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

3 April 2017

£12,000

DPA – 1st Principle, 2nd Principle

(PECR – Regulation 22 also considered, but was not a basis for the monetary penalty)

Factual background

The National Society for the Prevention of Cruelty to Children ('NSPCC') is a charity campaigning and working in child protection in the United Kingdom, the Channel Islands and the Isle of Man.

Collection and use of data

From June 2014 until August 2015, the NSPCC used a standard form (the 'June 2014 Form') when collecting the personal data of individuals. The June 2014 Form did not provide any privacy

information about the use of the personal data collected for live telephone or mail marketing. In each case, some time after the collection of the data, the NSPCC sent the individuals a letter which stated that their data would be used for marketing.

NSPCC collected personal data from 22,608 individuals using the June 2014 Form. Of these:

- 22,354 individuals were sent a total of 144,317 marketing mailings since June 2014;
- the personal data of 20,370 individuals were being used for mail marketing as of November 2016, with four complaints having been received; and
- 11,360 individuals received a total of around 22,720 live telephone marketing calls up to November 2016. 2,540 of the telephone numbers called were registered with the Telephone Preference Service ('TPS'), and 3,527 marketing calls were made to those numbers.

The TPS is a register of numbers allocated to subscribers who have notified the TPS that they do not wish to receive unsolicited calls for direct marketing purposes on those lines.

Data-matching and tele-matching

The NSPCC used the services of external companies to undertake data-matching and tele-matching on its behalf since at least 2010. Data-matching is the use of personal data to obtain and use other items of personal data which data subjects may have chosen not to provide to the data controller, and tele-marketing is a data-matching by which telephone numbers are obtained and used. From 6 April 2010 until May 2016 the NSPCC tele-matched 246,751 individuals' records in order to obtain their telephone numbers and make marketing calls to them. 46,415 telephone numbers were on the TPS, but the NSPCC did not screen the numbers against the TPS. From May 2016 onwards the NSPCC tele-matched numbers for data accuracy purposes. The NSPCC also used the services of an external company to match email addresses to individual supporter records. In November 2014 the NSPCC data-matched 115,741 individuals' email addresses to the personal data of supporters.

Wealth screening

The NSPCC used the services of a wealth screening company to market specific events to a select number of appropriate individuals. The personal data which the NSPCC provided to the wealth screening company included supporters' names and addresses and information relating to their donation history.

The wealth screening company appended 3,217 records, of the 2,105,145 screened, with a specific 'millionaire' wealth flag. In April 2015 the NSPCC contacted 493 of these 3,217 individuals across two fundraising communications specifically on the basis of that wealth flag. The NSPCC also used the services of a wealth screening company to screen 5,870,135 supporter records held in data warehouses, although these included duplicate supporter records, as the same supporter may have been included on multiple databases. It appended 1,862 of these records with a wealth flag, and selected 70 of these for a regional legacy event.

'You Can' Direct Response Television campaign

In June 2014 the NSPCC began its 'You Can' Direct Response Television ('DRTV') campaign. The campaign ended in November 2015. Individuals who made a donation by text received two separate bounce-back text messages. As of June 2016, 73,921 individuals had made a donation via SMS text to the NSPCC as part of this campaign, and received two bounce-back text messages in response:

'Thank you for supporting the NSPCC. We'd like to contact you to tell you more about our work. For terms visit <http://www.nspcc....>'

'Text OUT to 70744 to stop further contact'

The Commissioner considers that these bounce back text messages were sent for the purposes of direct marketing since they informed supporters of the NSPCC's intention to make further marketing approaches in the future. Further, individuals were automatically opted-in to receive further marketing communications.

ICO finding

The ICO was satisfied that the contraventions of the Data Protection Act 1998 ('DPA') were deliberate, in the sense that the actions of the NSPCC were deliberate. While the NSPCC may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. The ICO also found that the NSPCC failed to take reasonable steps to prevent the contraventions of the DPA from occurring.

Collection and use of data

The ICO found that the NSPCC's system of processing personal data was unfair because it did not inform individuals that their data would be processed for the purposes of live telephone or mail marketing at the time the data was collected and/or before the intended processing occurred (DPA – 1st Principle, 2nd Principle).

Data-matching and tele-matching

The ICO also found that it was unfair for the NSPCC to use the data for data-matching and/or tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

Wealth screening

The ICO found that the NSPCC unfairly processed individuals' personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that NSPCC would adopt these techniques (through the NSPCC's privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

'You Can' Direct Response Television campaign

The ICO considered that the bounce back text messages were sent for the purposes of direct marketing because they informed supporters of the NSPCC's intention to make further marketing approaching in the future and the NSPCC had failed to receive the necessary consent for such direct marketing (PECR – Regulation 22). This contravention was recorded by the ICO as an additional matter of concern but was not used as a basis for the MPN.

Harm

The ICO considered that the contraventions of the DPA were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the individuals' were effectively stripped of control over their own personal data (where the NSPCC used the June 2014 Form) or the data subjects were likely to have been affected by those contraventions in significant practical ways (where data-matching and wealth screening took place).

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
 - at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from the NSPCC; and
 - given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage.
- Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- The NSPCC had followed the unlawful practices described above over a period of several years and on a continuing basis.
- The NSPCC's practices appear to have been driven at least in part by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- The NSPCC had contravened the fundamental rights of a very large number of individuals not to be subject to unlawful direct telephone marketing and to have their personal data processed in accordance with the DPA and Directive 95/46/EC.
- By failing adequately to explain to data subjects how their personal data would be used, the NSPCC had deprived them of control and informed decision-making about their personal data to a significant extent.
- The NSPCC's activities as described above have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to unsolicited direct marketing communications. It is likely that many individuals will have been persuaded by the NSPCC to increase their financial support. Those financial consequences will to a significant extent have flowed from the NSPCC's unlawful practices described above.
- It is likely that the NSPCC has also contravened Regulation 22 of PECR.

Mitigating factors

- The NSPCC co-operated with the Commissioner's investigations.
- The NSPCC is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- The NSPCC has taken remedial action.
- The NSPCC's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

3 April 2017

£14,000

DPA – 1st Principle, 2nd Principle

Factual background

Macmillan Cancer Support ('Macmillan') is one of the largest British charities and provides specialist health care, information and financial support to people affected by cancer.

Wealth screening

Macmillan used the services of wealth screening companies to analyse the financial status of its supporters in order to identify wealthy or high value individuals. The personal data which Macmillan provided to the wealth screening companies included supporters' names and addresses and information relating to their donation history. The wealth screening companies then analysed the data in order to identify wealthy or high value individuals amongst Macmillan's donors. Macmillan confirmed that it had undertaken such activity in respect of donors on its database on two occasions, in 2009 and 2014. In 2014 details of 2,188,508 of its supporters had been processed for the purposes of wealth analysis.

Tele-matching

Macmillan also used the services of an external company to undertake tele-matching on its behalf since 2009. The ICO understood that, while Macmillan does not hold records of the precise number of data subjects involved, it is likely to be several hundred thousand.

ICO finding

The ICO was satisfied that these contraventions were deliberate, in the sense that the actions of Macmillan were deliberate. Alternatively, Macmillan ought reasonably to have known that there was a risk that the contraventions would occur, and that they would be of a kind likely to cause substantial damage or distress.

Wealth screening

The ICO found that Macmillan unfairly processed individuals' personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that NSPCC would adopt these techniques (through the Macmillan's privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

Tele-matching

The ICO also found that it was unfair for Macmillan to use the data for data-matching and/or tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

Harm

The ICO considered that the contraventions were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from Macmillan; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- Macmillan followed the unlawful practices over a period of several years.
- Macmillan's practices appeared to have been driven by financial gain. Its charitable status was not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- Macmillan contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the Data Protection Act 1998 and Directive 95/46/EC.
- By failing adequately to explain to data subjects how their personal data would be used, Macmillan has deprived them of control and informed decision-making about their personal data to significant extent.
- Macmillan's activities have exposed the relevant data subjects to substantially distressing and/or damaging consequences.

Mitigating factors

- Macmillan co-operated with the ICO's investigations.
- Macmillan is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- Macmillan's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

3 April 2017

£16,000

DPA – 1st Principle, 2nd Principle

Factual background

Cancer Support UK ('CSUK') is a charity that provides practical and emotional support to people with cancer, during and after the treatment period.

CSUK shared the names and addresses of its supporters with third party organisations. CSUK also participated in the Reciprocate Scheme, a scheme run by an external company which enabled participating charities to share or swap the personal data of donors or prospective donors. The Commissioner understands that CSUK no longer shares personal data of its supporters in this way.

CSUK shared 3,075,550 records of its supporters between April 2010 and August 2016 with other organisations and charities through recognised list brokers who were 'DPA-compliant'.

ICO finding

The ICO found that CSUK did not process data fairly because the terms of CSUK's privacy notice did not provide data subjects with adequate information as to how their personal data would be shared with third parties (DPA – 1st Principle). The ICO also found that such sharing was incompatible with the purposes explained in CSUK's privacy notices (DPA – 2nd Principle).

In particular:

- CSUK failed to take reasonable steps to prevent these contraventions from occurring.
- CSUK did not amend its privacy notice adequately.

The ICO was satisfied that these contraventions were deliberate, in the sense that the actions of CSUK were deliberate. While CSUK may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so.

Alternatively, CSUK ought reasonably to have known that there was a risk that the contraventions would occur, and that they would be of a kind likely to cause substantial damage or distress.

Harm

The ICO considered these contraventions to be 'serious' due to the number of individuals affected, the duration of contravention, and potential consequences of the contravention.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed if their personal data is shared by one charity with another for the purposes of the latter's fundraising efforts, without it being made sufficiently clear to the data subject that this would happen;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with approaches from the bodies with which their data was shared; and

- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- CSUK had followed the unlawful practice over a period of several years.
- CSUK's practice appears to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- CSUK had contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the Data Protection Act 1998 and Directive 95/46/EC.
- By failing to adequately explain to data subjects how their personal data would be used, CSUK has deprived them of control and informed decision-making about their personal data to a significant extent.
- CSUK's activities exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to increased direct marketing communications from CSUK and/or other charities. It is likely that many individuals will have been persuaded – by CSUK and/or other charities – to increase their financial support. Those financial consequences will to a significant extent have flowed from CSUK's unlawful data protection practice.

Mitigating factors

- CSUK co-operated with the Commissioner's investigations.
- CSUK is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- CSUK's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

3 April 2017

£16,000

DPA – 1st Principle, 2nd Principle

Factual background

Wealth screening

Cancer Research UK ('CRUK') used the services of a wealth screening company to analyse the financial status of its supporters in order to identify those that would have the capacity and propensity to make a larger donation to charity. The personal data which CRUK provided to the wealth screening company included supporters' names and addresses and information relating to their donation history. Between 2010 and 2016, CRUK processed 10,017,997 records for the purposes of wealth analysis relating to 3,523,566 supporters.

Tele-matching

CRUK also used the services of external companies to undertake tele-matching (tele-marketing is a data-matching by which telephone numbers are obtained and used) on its behalf. Since July 2011 it has matched at least 678,887 telephone numbers to supporters for whom it has other personal data.

ICO finding

The Commissioner was satisfied that these contraventions were deliberate, in the sense that the actions of CRUK were deliberate. While CRUK may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. Alternatively, CRUK ought reasonably to have known that there was a risk that the contraventions would occur, and that they would be of a kind likely to cause substantial damage or distress.

Wealth screening

The ICO found that CRUK unfairly processed individuals' personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that CRUK would adopt these techniques (through CRUK's privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

Tele-matching

The ICO also found that it was unfair for CRUK to use the data for data-matching and/or tele-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

Harm

The ICO considered that the contraventions were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from CRUK; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- CRUK has followed the unlawful practices over a period of several years.
- CRUK's practices appear to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- CRUK has contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the Data Protection Act 1998 and Directive 95/46/EC.
- By failing to adequately explain to data subjects how their personal data would be used, CRUK has deprived them of control and informed decision-making about their personal data to a significant extent.
- CRUK's activities have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including intrusions into their privacy due to increased direct marketing communications from CRUK. It is likely that many individuals will have been persuaded by CRUK to increase their financial support. Those financial consequences will to a significant extent have flowed from CRUK's unlawful data protection practices.

Mitigating factors

- CRUK co-operated with the Commissioner's investigations.
- CRUK is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- CRUK has taken remedial action.
- CRUK's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

3 April 2017

£9,000

DPA – 1st Principle, 2nd Principle

Factual background

Battersea Dogs & Cats Home ('BDCH') is an animal shelter which rescues cats and dogs in need of help, and nurtures them until an owner or a new home can be found.

BDCH used the services of external companies to undertake tele-matching on its behalf between November 2010 and July 2015. Tele-matching is the use of personal data to obtain and use telephone numbers which data subjects may have chosen not to provide to the data controller. The ICO understands that in the period between January 2011 and July 2015 BDCH processed a total of 740,181 records containing personal data for this purpose. This resulted in 385,709 records being matched and 229,476 individuals being contacted.

ICO finding

The ICO considered that BDCH's privacy notices in place at the relevant time did not indicate that personal data would be used for tele-matching purposes. The ICO found that BDCH did not process its supporters' personal data fairly because BDCH did not have the required consent to use the data for tele-matching purposes and such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st and 2nd Principles).

In particular, BDCH did not amend its privacy notices adequately, or obtain consent from the data subjects to the processing of data for tele-matching purposes.

The ICO is satisfied that these contraventions were deliberate, in the sense that BDCH's actions were deliberate. While BDCH may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. Alternatively, BDCH ought reasonably to have known that there was a risk of these contraventions occurring, and that they would be of a kind likely to cause substantial damage or distress.

Harm

The ICO was satisfied that the contraventions identified were 'serious' due to the duration of the contravention, the number of individuals affected, and potential significant consequences of the contravention, which included receiving additional marketing communications from BDCH and/or marketing communications using contact details which the data subjects may have declined to provide.

The ICO held that the contraventions were of a kind likely to cause substantial damage or substantial distress to the individuals concerned, taking into account:

- At least some proportion of data subjects are likely to be distressed if BDCH uses personal data they have chosen to provide in order to obtain and use data which they have chosen not to provide, in order to contact them for direct marketing purposes. They are also likely to be distressed by not being told in advance that their personal data may be used in that way.
- At least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional marketing approaches from the BDCH arising from its tele-matching practices.

- Given the scale and duration of the contravention, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- BDCH followed the unlawful practice described over a period of several years.
- practice appears to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
- BDCH has contravened the fundamental rights of very large numbers of individuals to have their personal data processed in accordance with the Data Protection Act 1998 and Directives 95/46/EC.
- By failing to adequately explain to data subjects how their personal data would be used, BDCH has deprived them of control and informed decision-making about their personal data to a significant extent.
- BDCH's activity has exposed the relevant data subjects to substantially distressing and/or damaging consequences, including: intrusions into their privacy due to increased direct marketing communications from BDCH. It is likely that many individuals will have been persuaded to increase their financial support. Those financial consequences will to a significant extent have flowed from BDCH's unlawful data protection practice.

Mitigating factors

- BDCH co-operated with the ICO's investigations.
- BDCH is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- BDCH's practice may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- BDCH has taken remedial action.
- The intended monetary penalty may have negative reputational consequences for BDCH.

3 April 2017

£11,000

DPA – 1st Principle, 2nd Principle

Factual background

Great Ormond Street Hospital Children's Charity ('GOSHCC') is an academic medical research centre specialising in paediatrics.

Sharing personal data with third parties

Between 2011 and September 2015, GOSHCC participated in the Reciprocate Scheme. During this period the GOSHCC disclosed batches of records containing unique reference numbers; names; addresses; last donation amount, Gift Aid status; and information about donation type. In total, GOSHCC disclosed 910,283 batches of records containing personal data to around 40 other charities while participating in the scheme.

Wealth screening

GOSHCC also used the services of a wealth screening company to run two campaigns to analyse the financial status of its supporters in order to identify those that would have the capacity and propensity to make a larger donation, and to predict whether they were likely to leave a legacy. The personal data which GOSHCC provided to the wealth screening company included supporters' names, telephone numbers and email addresses. Between April 2010 and June 2016 it had processed on average 795,000 records for the purposes of wealth screening per month.

Data-matching

Between 2012 and 2015, GOSHCC used the services of an external company to match email addresses to individual supporters' records. GOSHCC matched 103,500 email addresses to the personal data of supporters. GOSHCC also matched 208,000 dates of birth to individual supporters' records.

ICO finding

The ICO was satisfied that the contraventions were deliberate, in the sense that the actions of GOSHCC were deliberate. While GOSHCC may not have deliberately set out to contravene the DPA, it deliberately acted in such a way that it did so. The ICO also found that GOSHCC failed to take reasonable steps to prevent the contraventions of the DPA from occurring.

Sharing personal data with third parties

The ICO found that GOSHCC unfairly processed individuals' personal data because the terms of its privacy notice were unduly vague and/or ambiguous and did not provide data subjects with adequate information as to how their personal data would be shared via the schemes (DPA – 1st Principle). The ICO also found that the sharing of personal data via the schemes was incompatible with the purposes explained in GOSHCC's privacy notices (DPA – 2nd Principle).

Wealth screening

The ICO found that GOSHCC unfairly processed individuals' personal data because using their data to perform wealth screening was not in the reasonable expectation of those individuals and they were not informed that GOSHCC would adopt these techniques (through GOSHCC's privacy policy or otherwise) (DPA – 1st Principle). The ICO also found that the purpose of wealth analysis was incompatible with the purposes for which the data were obtained (administering the donation, and if the individual consented, for marketing purposes) (DPA – 2nd Principle).

Data-matching and tele-marketing

The ICO found that it was unfair for GOSHCC to use the data for data-matching purposes without consent of the data subjects and that such activities were incompatible with the purposes explained in their privacy notices (DPA – 1st Principle, 2nd Principle).

Harm

The ICO considered that the contraventions were serious because of the length of time over which the contraventions took place, the number of data subjects whose rights were infringed and the data subjects were likely to have been affected by those contraventions in significant practical ways.

The ICO was satisfied that these contraventions were of a kind likely to cause substantial damage or substantial distress, taking into account that:

- at least some proportion of data subjects are likely to be distressed as a result of the contravention;
- at least some proportion of data subjects are likely to suffer a financial impact and a diversion of time and resources in dealing with additional approaches from GOSHCC; and
- given the scale and duration of the contraventions, it is likely that such distress and/or damage would be substantial. At least some of the affected data subjects would have been likely to suffer substantial distress and/or damage. Alternatively, the cumulative levels of damage and/or distress of this kind of contravention would have been likely to be substantial.

Aggravating factors

- GOSHCC had engaged in the unlawful practices over a period of several years.
- GOSHCC's practices were driven by financial gain, this is aggravated by the fact that the public may expect charities to be especially vigilant in complying with their legal obligations.
- GOSHCC had contravened the fundamental right of data subjects to have their personal data processed in accordance with the Data Protection Act 1995 and Directive 95/46/EC.
- By failing to adequately explain to the data subjects the manner in which their personal information would be processed, GOSHCC had deprived the individuals of control and informed decision making about their personal data.
- GOSHCC's activities exposed the relevant data subjects to substantially distressing consequences, including intrusions into their privacy due to increased direct marketing communications. It is likely that many individuals will have been persuaded by GOSHCC to increase their financial support. Those financial consequences will to a significant extent have flowed from GOSHCC's unlawful data protection practices.

Mitigating factors

- GOSHCC co-operated with the Commissioner's investigations.
- GOSHCC is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
- GOSHCC took remedial action.
- GOSHCC's practices may to an extent have reflected commonplace – albeit mistaken and unlawful – approaches in the charitable sector.
- The intended monetary penalty may have negative reputational consequences.

Monevo Limited

13 April 2017

£40,000

PECR – Regulation 22

Factual background

Monevo Limited (Monevo) is a financial brokerage company which offers to find lenders and financial service providers for applicants via an online service. Monevo engaged a third party to carry out a text marketing campaign on its behalf which directed recipients to a web link, which in turn redirected to the website of 'Purple Payday', a trading name of Monevo. 353,740 such text messages were sent.

44,172 of these text messages were sent using data obtained from three competition or money saving websites. The privacy notices on those websites were generic and unspecific and none indicated that the data would be used for sending direct marketing text messages by or on behalf of the company.

Between the dates of 1 April 2016 and 28 June 2016 GSMA's Spam Reporting Service received 130 complaints in relation to the text messages sent on behalf of Monevo.

ICO finding

The ICO found that in contracting with the affiliate company to send the direct marketing text messages on its behalf, Monevo instigated the sending of the text messages, regardless of whether or not the text messages had been in the form agreed.

As the instigator, it was Monevo's responsibility to ensure that the necessary consent had been gained. The ICO was satisfied that Monevo did not have the consent of the 44,172 subscribers to whom it instigated the sending of unsolicited direct marketing messages (Regulation 22 of PECR).

In particular, Monevo:

- failed to take reasonable steps to prevent the contraventions; and
- did not carry out any, or any sufficient, due diligence to satisfy themselves that the third party affiliate had obtained the data it is using fairly and lawfully, and that they have the necessary consent.

The Commissioner did not consider this contravention deliberate, but the Commissioner was satisfied that Monevo knew or ought reasonably to have known that there was a risk that these contraventions would occur.

Harm

The ICO was satisfied that the contravention was 'serious' owing to the number of individuals affected and the number of complaints received.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Construction Materials Online Ltd

26 April 2017

£55,000

DPA – 7th Principle

Factual background

Construction Materials Online Ltd ('CMO') operated a website that had been developed by a third party company. The website enabled its customers to purchase building products online by entering their card details which were then encrypted and sent directly to an external payment system. However, CMO were unaware that the login pages contained a coding error.

An attacker exploited this vulnerability and gained access to usernames and passwords. The attacker uploaded a 'malicious web shell' to further compromise the system and on 6 May 2014 was able to modify payment pages and access 669 unencrypted cardholder details at the point of entry to the website. This included names, addresses, primary account numbers and security codes.

ICO finding

The ICO found that although CMO did not deliberately contravene the DPA, CMO failed to take appropriate technical measures against the unauthorised or unlawful processing of personal data (DPA – 7th Principle). This was a serious oversight.

The ICO found that CMO ought reasonably to have known that there was a risk of an attack occurring which was likely to cause substantial damage or distress unless the data processed on its website was appropriately protected.

Harm

The ICO found that owing to the number of data subjects, nature of the information which was stolen and potential consequences, the attack was 'serious'.

The ICO found that there was a risk the contravention would be of a kind likely to cause substantial damage or distress, particularly as the information was misused by the person who had access to it, exposing the customers to fraud.

Aggravating factors

- CMO was not aware of the security breach until notified by a customer.
- CMO received approximately 50 complaints and enquiries from its customers as a result of the security breach.

Mitigating factors

- CMO's website was subjected to a criminal attack.
- CMO notified the data subjects so that fraudulent transactions were intercepted.
- CMO was co-operative during the ICO's investigation.
- CMO took substantial remedial action.
- A monetary penalty might have a significant impact on CMO's reputation and to some extent its resources.

Greater Manchester Police

2 May 2017

£150,000

DPA – 7th Principle

Factual background

In 2015 Greater Manchester Police ('GMP') sent three unencrypted DVDs by Recorded Delivery to the Serious Crime Analysis Section ('SCAS'). The DVDs contained footage of police interviews with victims of serious violent or sexual crimes in ongoing cases. The victims were named and talking openly about the crimes.

The SCAS did not receive the DVDs and they have not been recovered.

ICO finding

The ICO found that GMP failed to take appropriate organisational measures against unauthorised or unlawful processing of personal data and against accidental loss of personal data (DPA – 7th Principle). GMP should have known or ought to have envisaged those risks and it did not take reasonable steps to prevent the loss.

The sending of similar DVDs by recorded delivery was an ongoing contravention from 2009 until this incident in 2015.

The ICO did not consider this contravention to be deliberate, however, the GMP should have known or ought to reasonably have known that there was a risk that this contravention would occur.

Harm

The ICO is satisfied that the contravention identified was 'serious' because the DVD's contained highly sensitive personal data. The ICO found that the loss of the DVDs was likely to cause substantial damage or distress to the victims. This included distress that their highly sensitive personal data could have been accessed by individuals who had no right to see that information. This could lead to further distress if that information was misused by untrustworthy third parties.

Aggravating factors

- The DVDs were not password protected.

Mitigating factors

- GMP referred the incident to the ICO and SCAS.
- GMP was cooperative during the investigation.
- As far as the ICO is aware, the information on the DVDs has not been further disseminated.
- GMP notified the affected individuals and provided support.
- GMP has taken remedial action until a technical solution can be found.
- A monetary penalty may have a significant impact on GMP's reputation.

Keurboom Communications Ltd

3 May 2017

£400,000

PECR – Regulation 19

Factual background

Keurboom Communications Ltd ('Keurboom') provides (among other things) telephony services including 'voice broadcasting' to companies in order to generate leads so that they can maximise their potential sales.

Between 29 April 2015 and 7 June 2016, the ICO received 1,036 complaints via its online reporting tool. The essence of the complaints was that automated marketing calls had been received by subscribers, mainly in relation to road traffic accidents and PPI claims. Some of the complainants had also received repeat calls (sometimes on the same day) and at unsocial hours.

The calls allowed an option to press 5 if interested, or an option to press 9 to be removed from the list. The calls did not identify the sender and the option of being connected to a person or suppressing the number was not always effective. Some of the calls were also misleading because they gave the impression that the calls were urgent and related to a recent road traffic accident or an ongoing PPI claim.

ICO finding

The Commissioner found that Keurboom instigated automated marketing calls to subscribers without their prior consent (Regulation 19 of PECR).

Between 1 October 2014 and 31 March 2016, Keurboom sent or instigated 99,535,654 automated marketing calls to subscribers without their prior consent.

The ICO also found that Keurboom's actions which constituted the contravention were deliberate actions (even if Keurboom did not actually intend thereby to contravene PECR).

Harm

The ICO was satisfied that the contravention identified was 'serious' because of the number of individuals affected and the extent of the contravention.

Aggravating factors

- Keurboom did not co-operate with the Commissioner's investigation.
- Keurboom might obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.

Mitigating factors

- There were no mitigating features

Onecom Limited

11 May 2017

£100,000

PECR – Regulation 22

Factual background

Onecom confirmed that it had sent 3,284,908 text messages between 1 October 2015 and 31 March 2016. Of these, 2,796,075 had been received by the recipient. The data used by Onecom for sending the marketing text messages had been obtained from various sources: (i) data acquired through the acquisition of other businesses; (ii) data obtained by Onecom from its own customers; and (iii) data obtained from third party data suppliers.

Between 26 October 2015 and 2 June 2016, 1050 complaints were made to GSMA's Spam Reporting Service, or directly to the ICO, about the receipt of unsolicited direct marketing text messages relating to mobile phone upgrades. The GSMA's Spam Reporting Service allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA, who makes such complaints data available to the ICO. 944 of such messages did not identify Onecom as the sender, though the ICO was satisfied that all 1050 text messages complained about were sent by Onecom. Onecom was unable to provide evidence that it had consent to send those text messages or that it could rely on the 'soft opt-in'.

ICO finding

The ICO found that Onecom sent direct marketing messages without the appropriate consent (Regulation 22 of PECR).

The Commissioner did not consider the contravention deliberate but Onecom should have known or ought to reasonably have known that there was a risk that this contravention would occur. The ICO found that Onecom had failed to take reasonable steps to prevent the contravention.

Harm

The Commissioner was satisfied that the contravention identified was 'serious' because of the number of individuals affected by the contravention.

Aggravating factors

- Onecom contravened regulation 23 of PECR in that it did not (at the very least in 944 of the 1050 text messages complained of) identify the person on whose behalf the messages were sent.

Mitigating factors

- Onecom has stopped sending marketing texts and taken a number of remedial steps to ensure future compliance.

Brighter Home Solutions Ltd

12 May 2017

£50,000

PECR – Regulation 21

Factual background

Brighter Home Solutions' ('BHS') business involves making marketing calls to subscribers in order to sell its home improvement products and services including windows, doors, conservatories and kitchens.

Between 4 January 2016 and 26 August 2016, the Telephone Preference Service ('TPS') received 160 complaints about BHS. The TPS is a register of numbers allocated to subscribers who have notified the TPS that they do not wish to receive unsolicited calls for direct marketing purposes on those lines. The TPS referred all of those complaints to BHS and also notified the ICO. BHS did not respond to the TPS in relation to any of the complaints.

Some of the individual subscribers complained that the calls were misleading because the callers gave the impression that they were calling from a local number and were misled into believing that they may have been contacted by BHS previously and agreed at that time to receive further calls in the future.

After being contacted by the ICO, BHS explained that it purchased opt-in data from third party companies, which it then used to call individual subscribers to market its products and services. However, BHS hadn't carried out any due diligence checks to ensure that the individual subscribers had given their consent to BHS to receiving such calls.

ICO finding

The ICO found that BHS made live marketing calls to subscribers who had registered with the TPS at least 28 days prior to receiving the calls and they had not given their prior consent to BHS to receive calls (Regulation 21 of PECR).

In particular:

- BHS was unable to provide any evidence that it had undertaken appropriate due diligence in this case.
- BHS was unable to provide sufficient evidence that the individuals to whom the text messages had been sent had consented to the receipt of those messages.

The ICO did not consider the contravention deliberate, but BHS failed to take reasonable steps to prevent the contravention and were therefore negligent.

Harm

The Commissioner was satisfied that the contravention was 'serious' because there were multiple breaches of regulation 21 by BHS over an 8 month period, which led to a significant number of complaints to the TPS and the ICO.

Concept Car Credit Limited

12 May 2017

£40,000

PECR – Regulation 22

Aggravating factors

- BHS might obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
- BHS misled subscribers by displaying a false CLI (Calling Line Identification) that had the same area code as the subscriber. This led subscribers to think that the call was from someone in their local area. This was done as the subscriber was more likely to answer the telephone.
- The call script used by BHS contained the misleading statement ‘... [we] are calling everyone back who did not receive our call or who may have asked us to call back this year. It was a while back so don’t worry if you do not remember receiving the call.’ This was not necessarily always the case.
- In October 2016 the ICO received evidence that although BHS had an up to date TPS registration, it had not accessed the system for at least the previous 4 months. As such, there was no evidence that company had screened its data against the TPS in order to avoid callings subscribers who did not wish to be called.

Mitigating factors

- There was a potential for damage to BHS’s reputation which may affect future business.

Factual background

Concept Car Credit Limited (the ‘Company’) is a used car dealer offering both cars for sale and brokering car finance.

Over an 18 month period between 2015 and 2016, the Company used a public telecommunications service for the purposes of instigating the transmission of 336,000 unsolicited communications by means of text message to individual subscribers for the purposes of direct marketing.

Between 9 April 2015 and 5 March 2016, 66 complaints were made to GSMA’s Spam Reporting Service, or direct to the ICO, about the receipt of unsolicited direct marketing text messages sent on behalf of the Company. The GSMA’s Spam Reporting Service allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA, who makes such complaints data available to the ICO.

The Company explained that it had obtained the data used to send the text messages from a number of third parties with whom they hold introducer agreements between 2012 and 2016. However, the Company was unable to provide sufficient evidence that the individuals to whom the text messages had been sent had consented to the receipt of those messages.

ICO finding

The ICO found that the Company did not have the consent of the 336,000 subscribers to whom it had instigated the sending of unsolicited direct marketing text messages (PECR – Regulation 22).

In particular:

- The Company was unable to provide any evidence that it had undertaken appropriate due diligence in this case.
- The Company was unable to provide sufficient evidence that the individuals to whom the text messages had been sent had consented to the receipt of those messages.
- The Company failed to take reasonable steps to prevent the contraventions in this case.

The Commissioner was satisfied that the contravention was not deliberate, however, the Company knew or ought reasonably to have known that there was a risk that these contraventions would occur.

Harm

The ICO considered the contravention ‘serious’ because there were multiple breaches of Regulation 22 of PECR by the Company over an 18-month period. In addition, a large number of complaints were made to the ICO and GSMA’s Spam Reporting Service.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

22 May 2017

£150,000

DPA – 7th Principle

Factual background

Basildon Borough Council (the ‘Council’) is a local planning authority which is required to make decisions on planning applications. This involves its planning department uploading planning applications to its website in order to consult with the public.

On 16 July 2015, an administrator in the Council’s business services department received a planning statement (the ‘statement’) in support of a householder’s application for proposed works in a green belt. The statement contained sensitive personal data relating to a static traveller family (the ‘family’) that had been living on the relevant site for many years. In particular, the statement referred to the family’s disability requirements, including mental health issues, the names of all the family members, their age and the location of the site.

The Council’s policy and established approach was that personal would be redacted from such documents before being uploaded to the website. The planning technician, however, was inexperienced in checking the contents of documents relating to planning applications which contained sensitive information. He did not notice the information about the family that was embedded in the statement and therefore did not make any redactions. No procedure was in place for a second person to check such documents before they were uploaded. Consequently, the planning application, which contained sensitive personal data was uploaded onto the Council’s website on 16 July 2015 and remained available until it was removed on 4 September 2015.

ICO finding

The ICO found that the Council failed to take appropriate organisational measures against the unauthorised processing of personal data (DPA – 7th Principle). Basildon did not have in place appropriate organisational measures for ensuring so far as possible that such an incident would not occur, i.e. for ensuring that statements containing sensitive personal data would not be published on Basildon’s website. In particular, the Council did not:

- have in place an adequate procedure governing the redaction of statements by planning technicians;
- provide any (or any adequate) training to planning technicians on the redaction of statements;
- have in place any guidance or procedures for a second planning technician or senior officer to check statements for unredacted data (and specifically sensitive personal data) before they were returned to the administrator; and
- have in place any guidance for the administrator to check statements for unredacted data before they were uploaded to its website.

The Council had submitted that (i) it was obliged under the Town and Country Planning (Development Management Procedure) (England) Order 2015 (the ‘2015 Order’) to include the full contents (including any unredacted planning statements) of any application as part of its local authority planning register and (ii)

where it chose to make its planning register available it has no power to redact any details of its register. The ICO rejected these submissions for the following reasons:

- The 2015 Order could not be construed so as to oust an individual’s rights under the Data Protection Act 1998, Directive 95/46/EC or Article 8 of the European Convention on Human Rights;
- The Council’s duty to make the planning application available to members of the public did not entail including every single item of information which is included in the application;
- Disclosure on a website is materially different from a right of inspection, and where the Council chooses to make its planning register available it cannot override individuals’ rights under the Data Protection Act 1998, Directive 95/46/EC or Article 8 of the European Convention on Human Rights; and
- If every single item of information submitted with a planning application should have been made publicly available on its website, this should have been made clear to applicants so that they could make informed decisions about what data to include in their applications.

The Commissioner considers that Basildon did not deliberately contravene the DPA, but rather the contravention was the result of serious oversight. Basildon knew or ought reasonably to have known that there was a risk that this contravention would occur.

Harm

The Commissioner found that the contravention was ‘serious’ due to the number of affected individuals, the sensitive nature of the personal data that was contained in the statement, the period of time for which this sensitive personal data was available online and the potential consequences for the affected individuals. The Commissioner also found the contravention was of a kind likely to cause substantial distress and/or damage, because sensitive personal data was published online for six weeks and Basildon failed to process the personal data in accordance with its own policies and within reasonable expectations of the individuals.

Aggravating factors

- Basildon did not notify the affected individuals.
- Basildon had not taken sufficient remedial action.

Mitigating factors

- Basildon referred this incident to the Commissioner, removed the relevant data from its website and was co-operative during the Commissioner’s investigation.
- A monetary penalty might have a significant impact on Basildon’s reputation.
- Some of the personal data and sensitive personal data which Basildon should have redacted was otherwise available in a public document, namely the previously published report of a Planning Inspector.
- The affected individuals do not appear to have become aware of or complained about this contravention. The Commissioner was not aware of the affected individuals actually suffering any damage or distress in this case.

Gloucester City Council

26 May 2017

£100,000

DPA – 7th Principle

Factual background

On 17 April 2014 the Council's IT staff identified a vulnerability in its own systems when using an appliance known as 'SonicWall'.

A software patch for the vulnerability was available by the time of discovery, but the Council's third party IT outsourcers overlooked it and therefore the software patch was not applied.

In July 2014, Senior Officers of the Council had their Twitter accounts compromised by an attacker who also gained access to 16 user mailboxes via the vulnerability in the SonicWall appliance. The attacker was able to download 30,000 emails from these mailboxes which contained financial and sensitive personal information on approximately 40 members of current or former staff.

ICO finding

The ICO found that the Council failed to take appropriate technical and organisational measures for ensuring that emails containing financial and sensitive personal information could not be accessed (DPA – 7th Principle). In particular, the Council did not have a process in place to ensure that during outsourcing of its IT services the software watch was applied.

Harm

The ICO found that the Council's current or former staff had an expectation that their financial and sensitive personal data would have been held securely and that the Council's failure to do so had likely caused distress to the affected current and former staff.

The ICO also found that as the attacker had not been identified and the emails had not been recovered, further disclosure was possible and could cause damage as well as additional distress.

Aggravating factors

- The Council was not aware of the incident until the attacker notified it.
- The attacker had the option to download even more emails if they had chosen to do so.

Mitigating factors

- The Council's website was subject to a criminal attack.
- The Council reported the incident to the ICO and was co-operative during the investigation.
- The Council has taken significant remedial action.
- The intended monetary penalty may have a significant effect on the Council's reputation and (to some extent) its resources.

Boomerang Video Ltd

9 June 2017

£60,000

DPA – 7th Principle

Factual background

Boomerang Video operates a website that enables its customers to rent video games via a payment web application. The website was developed in 2005 by a third party company (the 'data processor'). The login page on the website contained a coding error Boomerang Video was unaware of.

On 5 December 2014, an attacker exploited this vulnerability by using SQL injection to gain access to usernames and password hashes for the WordPress section of the site. One password was shown to be a simple dictionary word based on the company's name. The attacker then uploaded a malicious web shell onto the web server to further compromise the system and gain access to the personal data of individuals stored within. On 30 December 2014, the attacker was able to query the customer database and download text files containing 26,331 cardholder details (including name, address, primary account number, and expiry date and security code). Although part of the primary account numbers were stored unencrypted, the attacker was able to gain access to the decryption key with ease, using information in configuration files on the web server. Industry guidelines prohibit the storage of the security code after payment authorisation.

This was an ongoing contravention from 2005 when the website was developed by the data processor until Boomerang Video took remedial action on 12 January 2015.

ICO finding

The ICO found that Boomerang Video failed to take appropriate technical measures against the unauthorised or unlawful processing of personal data (DPA – 7th Principle).

The Commissioner also found that Boomerang Video did not have in place appropriate technical measures for ensuring the personal data stored on the customer database could not be accessed by an attacker performing an SQL injection attack. In particular Boomerang Video failed to:

- carry out regular penetration testing on its website that should have detected the error;
- ensure that the password for the WordPress account was sufficiently complex to be resistant to a brute-force attack on the stored hash values; and
- keep the decryption key secure and prevent it being accessed by the attacker.

The Commissioner did not consider the contravention deliberate, but Boomerang Video ought reasonably to have known that there was a risk an attack performed by SQL injection would occur unless it ensured the personal data stored on the database was appropriately protected.

12 June 2017

£10,500

PECR – Regulation 22

Harm

The Commissioner considered Boomerang Video's failure to take adequate steps to safeguard against unauthorised or unlawful access 'serious' due to the number of data subjects, the nature of the personal data that was stored on the database and the potential consequences.

The Commissioner also found that the contravention was of a kind likely to cause substantial distress because of the number of data subjects and the nature of the personal data stored on the customer database. Further, ICO found that contravention caused damage because this information was misused by the person who had access to it, and exposed some of the data subjects to fraud.

Aggravating factors

- Boomerang Video was not aware of this security breach until 9 January 2015 when it was notified by its customers.
- Boomerang Video assessed itself to be compliant with the "Payment Card Industry Data Security Standard" despite failing to carry out penetration testing on its website.
- Boomerang Video received approximately 1,100 complaints and enquiries as a result of this security breach.

Mitigating factors

- Boomerang Video's website was subjected to a criminal attack.
- Boomerang Video reported this incident to the Commissioner and was co-operative during the investigation.
- The data processor assured Boomerang Video that the payment security codes were not stored on the customer database.
- Boomerang Video has now taken substantial remedial action.
- A monetary penalty may have a significant impact on Boomerang Video's reputation (and to some extent) its resources.

Factual background

WM Morrison Supermarkets Plc ('Morrison's') is a national chain of supermarkets.

As a result of an update to its systems in early 2016, Morrison's received queries from customers stating that they were not receiving e-mails from Morrison's. It therefore made the decision to send "Your account details" e-mail to individuals who had previously opted out of marketing in relation to their Morrison's More card but had opted in to marketing for online groceries, advising them on how to update their marketing preferences.

Between 24 October 2016 and 25 November 2016, Morrison's instigated the transmission of 236,651 "Your account details" e-mails. Of those, 130,671 e-mails were successfully received.

ICO finding

The ICO found that Morrison's had sent 130,671 unsolicited communications by means of e-mail to individuals subscribers for the purposes of direct marketing without the necessary consent (Regulation 22 of PECR).

As the instigator of the e-mails, it was the responsibility of Morrison's to ensure that sufficient consent had been acquired. Morrison's was unable to evidence that the individuals to whom e-mails had been sent had consented to receipt of the messages.

The Commissioner considered that Morrison's deliberately contravened Regulation 22 of PECR because Morrison's was aware that the e-mail was being sent to individuals who had previously indicated that they did not consent to receive direct marketing in relation to their Morrison's More card. However, Morrison's sent these individuals emails despite its knowledge of its obligations under the Data Protection Act 1998 to respect such opt-outs.

Harm

The Commissioner was satisfied that the contravention was 'serious' because between 24 October 2016 and 25 November 2016 Morrison's knowingly sent a total of 130,671 direct marketing emails to subscribers without their consent.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Remedial Action

- No mention of remedial action.

MyHome Installations Limited

19 June 2017

£50,000

PECR – Regulation 21

Factual background

MyHome Installations Limited (the ‘Company’) provides home security and electrical installation products and services to members of the public.

Between 6 April 2015 and 9 September 2016, the ICO received 169 complaints about unsolicited direct marketing calls made by the Company. Of those, 138 complaints were made to the Telephone Preference Service (‘TPS’) (a register of numbers allocated to subscribers who have notified the ICO that they do not wish to receive unsolicited calls for direct marketing purposes), with a further 31 made direct to the ICO. All of these complaints were made by individual subscribers who were registered with the TPS.

The Company had purchased data from third party companies for the purpose of marketing, and relied on their data providers to deliver their promise of high quality, TPS cleansed data. The Company was unable to provide consent for the complaints made, in response to the ICO’s enquiries, as the marketing manager in place at the time had left the business. This previous manager had historically bought data and added it to the company’s call lists without any way of referencing its source.

ICO finding

The ICO found between 6 April 2015 and 9 September 2016, the Company used a public telecommunications service for the purposes of making 169 unsolicited calls for direct marketing purposes to subscribers where the number allocated to the subscriber in respect of the called line was a number registered with the TSP, contrary to regulation 21(1)(b) of PECR.

The ICO also found that the 169 complaints were made by subscribers who had registered with the TPS at least 28 days prior to receiving the calls and they had not given their prior consent to the Company to receive calls.

The ICO did not consider the contravention deliberate. However, because the Company knew that people were complaining about calls they were receiving, the ICO considered that it ought to have known the risk of contravening PECR. The ICO also found that the Company failed to take reasonable steps to prevent the contraventions.

Harm

The ICO considered that these contraventions were ‘serious’ because there had been multiple breaches of regulation 21 by the Company arising from its activities over an 18 month period, which led to a number of complaints about unsolicited direct marketing calls being made to the TPS and the ICO. Also, it is reasonable to suppose that considerably more calls were made by the Company because those who went to the trouble of complaining are likely to represent only a proportion of those who actually received calls.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Providence Personal Credit Limited

11 July 2017

£80,000

PECR – Regulation 22

Factual background

Between 6 April 2015 and 13 October 2015, 285 complaints about the receipt of unsolicited direct marketing text messages relating to online loans were made to GSMA’s Spam Reporting Service, which shares complaints data with the ICO. The direct marketing text messages were sent by third party affiliates on behalf of Providence Personal Credit Limited (‘PPC’).

Under the affiliate agreement, PPC agreed to provide text promoting its products and the affiliates would send the text as direct marketing text messages. Affiliates received a fee for each individual who subsequently entered into a credit agreement with PPC having clicked on the web link contained in the text message.

Between 6 April 2015 and 31 October 2015, one of the affiliate companies, Money Gap Group Ltd, sent 868,393 unsolicited direct marketing text messages promoting PPC. In the same period another affiliate company, Sandhurst Associates Ltd, sent 130,664 unsolicited direct marketing text messages promoting PPC.

The individuals to whom the text messages were sent had not consented to the receipt of such direct marketing by or on behalf of PPC. The privacy notices used by the affiliates did not name PPC or any of its trading names, nor did they indicate that the data would be used for sending direct marketing text messages on behalf of PPC.

ICO finding

The ICO found that PPC instigated the sending of direct marketing messages without the appropriate consent (Regulation 22 of PECR).

The Commissioner also found that PPC failed to take reasonable steps to prevent the contravention because as the instigator of the direct marketing text messages, it was the responsibility of PPC to ensure valid consent to send direct marketing text messages had been acquired. Reasonable steps in these circumstances could have included reviewing the privacy notices and consent wording relied on by the affiliate companies, ensuring that they were sufficiently specific to amount to valid consent for the sending of direct marketing text messages on behalf of PPC.

The Commissioner did not consider PPC’s contravention of regulation 22 of PECR deliberate, however, PPC knew or ought reasonably to have known that there was a risk that these contraventions would occur and was therefore negligent.

Harm

The Commissioner was satisfied that the contravention was ‘serious’ because PPC instigated the sending of at least 999,057 direct marketing text messages to subscribers without their consent.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Moneysupermarket.com Ltd

17 July 2017

£80,000

PECR – Regulation 22

Factual background

Moneysupermarket.com Ltd ('Moneysupermarket') is an online price comparison service.

In December 2016, the company sent an email to a consumer advising them that the terms and conditions of the service had been updated. The individual complained to the ICO, stating that they had previously opted out of Moneysupermarket's marketing emails.

The ICO informed Moneysupermarket that organisations cannot email individuals to consent to future marketing. Upon discussion with the ICO, Moneysupermarket confirmed that all of the customers sent the terms and conditions update email had previously opted out of receiving direct marketing emails. Further, Moneysupermarket was unable to evidence that any individuals contacted had subsequently consented to this marketing.

ICO finding

The ICO found that Moneysupermarket knowingly instigated the transmission of 6,788,496 unsolicited marketing communications without the appropriate consent (Regulation 22 of PECR).

The ICO also found that Moneysupermarket failed to take reasonable steps to prevent the contraventions in this case. The ICO further considers that these actions were deliberate, as Moneysupermarket was aware that the emails were being sent, and that these individuals had not consented to the direct marketing.

Harm

The ICO was satisfied that the contravention was 'serious' due to the number of marketing emails sent without consent, which totalled 6,788,496 emails.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

H.P.A.S. Limited t/a Safestyle UK

31 July 2017

£70,000

PECR – Regulation 21

Factual background

Safestyle's business involves making marketing calls to subscribers in order to sell its products and services, including windows and doors to homeowners.

Between 1 May 2015 and 31 December 2016, the Commissioner received 264 complaints about unsolicited direct marketing calls made by Safestyle. Of those complaints, 178 complaints were made to the TPS, with a further 86 made directly to the ICO. All of these complaints were made by individual subscribers who were registered with the Telephone Preference Service ('TPS'), a register of numbers allocated to subscribers who have notified the ICO that they do not wish to receive unsolicited calls for direct marketing purposes, and/or who had not given their prior consent to Safestyle to receive direct marketing calls.

On 18 January 2016, the Commissioner wrote to Safestyle explaining that the ICO and the TPS had received complaints from individual subscribers in relation to unsolicited calls. Safestyle explained that it only canvassed existing customers and enquirers who had provided their number requesting a quotation to follow up on interest expressed. Safestyle said that it did not screen against the TPS as that would prevent it from contacting customers who are registered but who have nonetheless invited contact for quotation and sales purposes. Safestyle indicated it operates a suppression list and adds the telephone numbers of anybody asking not to be called again. Safestyle also advised that it was revisiting the way it conducted marketing in order to improve its practice and procedures.

Safestyle underwent three periods of monitoring to determine whether there was a suitable reduction in the number of complaints being recorded. However, despite Safestyle's assurances of its continued commitment to preventing unwanted contact with its customers, the Commissioner continued to receive an unacceptable level of complaints.

ICO finding

The Commissioner found that Safestyle made unsolicited direct marketing calls without the appropriate consent (Regulation 21 of PECR).

The ICO also found that Safestyle failed to screen the numbers against the TPS, maintain an accurate suppression list, and otherwise failed to take reasonable steps to prevent the contravention. Whilst the Commissioner was satisfied that Safestyle had not set out to deliberately contravene PECR, it knew or ought to have known that its direct marketing activities would lead to a contravention and was therefore negligent.

Harm

The ICO held that the contravention was 'serious' due to the number of complaints made, and the extended period over which the contraventions occurred. No financial loss was experienced by those affected, however they did experience a diversion of resources and time in having to deal with the unsolicited calls, and in having to report these to the TPS and the ICO.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Laura Anderson Limited t/a Virgo Home Improvements

31 July 2017

£80,000

PECR – Regulation 21

Factual background

Virgo Home Improvements ('VHI') sells home improvement products and services to residential homes in England.

Between 6 April 2015 and 22 November 2016, the ICO received 440 complaints about separate unsolicited direct marketing calls made by VHI. VHI had purchased 500,000 telephone numbers from a third party list supplier between 2010 and 2014, and following this used their own data bases and a further purchase of 400,000 numbers to fuel its telemarketing activities. There were no contracts in place with the data suppliers, but Virgo say they were assured by the relevant companies that data was Telephone Preference Service ('TPS') screened prior to being provided to them. The TPS is a register of numbers allocated to subscribers who have notified the TPS that they do not wish to receive unsolicited calls for direct marketing purposes on those lines.

Virgo does not hold its own TPS license and does not screen against the TPS register. Virgo indicated that they operate an internal suppression list and adds to it the telephone numbers of anybody asking not to be called again. Virgo also advised that prior to 2010, all data had been recorded and stored in a paper format which has now been destroyed following its transfer to an electronic format. Virgo was therefore unable to provide evidence of consent or that it had undertaken the appropriate due diligence with its list providers.

ICO finding

The ICO found that VHI had made unsolicited calls for direct marketing purposes without the appropriate consent (Regulation 21 of PECR). The ICO considers that VHI had deliberately contravened Regulation 21 of PECR because VHI did not screen against the TPS, nor did it keep clear records of which individuals had consented to be called.

Harm

The ICO was satisfied that the contravention was 'serious' due to the large number of data subjects affected, and the duration of the contravention (spanning over a year). Furthermore, the ICO recognised that these calls were likely to have caused distress to some individuals, as many of the individuals had received repeated unsolicited calls and their opt-out requests were ignored. The ICO also highlighted the targeting of some vulnerable individuals, including the elderly, and anecdotally referenced instances of VHI repeatedly contacting grieving families.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

TalkTalk Telecom Group Plc

7 August 2017

£100,000

DPA – 7th Principle

Factual background

In 2002, TalkTalk's portal was designed and implemented. Wipro, which was acting as processor to resolve high level complaints and monitor and address network connectivity problems on TalkTalk's behalf, was given access to the portal. 40 individual users employed in Wipro's High Repeat Team had access to the personal data of between 25,000 to 50,000 TalkTalk customers at any point in time.

In September 2014, TalkTalk began receiving complaints from customers regarding scam calls purportedly from TalkTalk. Typically, the callers purported to be providing support for technical problems which had been detected. They were able to quote customers' addresses and TalkTalk account numbers.

TalkTalk commenced an initial security investigation and reported the matter to the ICO on 11 September 2014. In October 2014, TalkTalk commissioned a specialist investigation which identified three Wipro user accounts that had been used to gain unauthorised and unlawful access to the relevant personal data of up to 21,000 customers.

In November 2014, and in February, October and November of 2015, TalkTalk wrote to all of its customers warning them of potential scam calls and how to deal with them.

ICO finding

The ICO found that TalkTalk did not have the appropriate technical and organisational controls to prevent unauthorised or unlawful processing of personal data (DPA – 7th Principle).

The ICO also found that TalkTalk did not have controls in place to limit access to the customers whose accounts were being worked on to resolve network problems, or to allow for the exporting of the fields that were actually needed for Ofcom reporting. Further, Wipro employees were able to access the portal from any internet-enabled device. No controls were put in place to restrict such access to devices linked to Wipro.

The Wipro employees were able to make "wildcard" searches, view large numbers of customer records at a time and to export data to separate applications and files (although there is no evidence of any bulk download of this data). Those capabilities gave opportunities for the misuse of the relevant personal data. There was no adequate justification for those capabilities.

The ICO considered that TalkTalk knew or ought reasonably to have known that there was a risk that the contravention would occur, and be of a kind likely to cause substantial damage or substantial distress. The ICO further found that TalkTalk failed to take reasonable steps to prevent such a contravention.

7 August 2017

£70,000

PECR – Regulation 21

Harm

The ICO considered the contravention ‘serious’ because of the number of inadequacies in TalkTalk’s technical and organisational measures, the number of individuals affected, the nature of the personal data compromised, and the extent of the contravention.

In light of such inadequacies, some of the relevant personal data was likely to be misused in furtherance of fraud and/or other criminal activity. The relevant personal data was likely to help scammers (a) identify and contact target individuals and (b) pass themselves off as representatives of TalkTalk. Such communications were likely to result in at least some recipients providing their bank details to scammers and/or being defrauded and/or having their bank accounts used for money laundering. Those consequences would constitute substantial damage, and would be likely to cause substantial distress to at least some recipients, whether individually or cumulatively.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- TalkTalk was the victim of the malicious actions of a small number of individuals.
- TalkTalk proactively reported this matter to the Commissioner.
- TalkTalk took steps to minimise potentially harmful consequences, for example by immediately removing the offending Wipro employees’ access to the portal and alerting all of its customers to the potential for scam calls.
- There is no evidence that the affected customers (up to 21,000) suffered any damage or distress as a result of these incidents.
- TalkTalk has implemented certain measures to prevent the recurrence of such incidents.

Factual background

In 2012, Islington’s internal application team developed ‘TicketViewer’ on behalf of Islington Parking Services (‘the application’). It was hosted separately to Islington’s other systems. A user could log onto the application by entering the vehicle registration number (‘VRN’) and a parking ticket number to see a CCTV image or video of their alleged contravention or offence. If a user still wanted to appeal a parking ticket, they could send supporting evidence to Islington Parking Services by email or post. This included their name and address together with details of any mitigating circumstances such as health issues, disabilities and financial details. The back office processing centre scanned all of this information (including the parking ticket and the CCTV image or video that showed the VRN) onto the user’s ticket attachment folder.

On 25 October 2015, Islington was informed by a user that the ticket attachment folders could be accessed by manipulating the URL in the user’s browser. At that time, the ticket attachment folders contained personal data relating to approximately 89,000 users, including sensitive personal data and financial details. On 16 and 25 October 2015, external testing discovered that a total of 119 documents had been accessed a total of 235 times from 36 unique IP addresses affecting 71 individuals.

ICO finding

The ICO found that Islington failed to take appropriate technical measures against the unauthorised and unlawful processing of personal data (DPA — 7th Principle). The Commissioner did not consider the contravention to be deliberate, however, Islington ought reasonably to have known that there was a risk that that unauthorised or unlawful access would occur unless it ensured that the personal data held in the ticket attachment folders was appropriately protected.

The ICO also found that Islington failed to take reasonable steps to prevent the contravention, such as ensuring that Islington’s IT security team tested the application prior to going live, and regular testing subsequently.

Harm

The Commissioner is satisfied that the contravention was ‘serious’ due to the number of data subjects, the nature of the personal data that was held in some of the ticket attachment folders and the potential consequences. Further, the Commissioner considered that the contravention was of a kind likely to cause distress to the users if they knew that their personal data had been accessed by unauthorised individuals. The Commissioner also considers that such distress was likely to be substantial, having regard to the number of users and the nature of the data that was held in the ticket attachment folders.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- Islington referred this incident to the Commissioner, immediately took the application offline and was co-operative during the Commissioner’s investigation.
- The affected individuals were notified by Islington.
- The Commissioner is not aware of the affected individuals actually suffering any damage or distress in this case.
- A monetary penalty may have a significant impact on Islington’s reputation, and to an extent, its resources.
- This incident has been publicised on social media and in the local press.

15 August 2017

£50,000

PECR – Regulation 21

Factual background

Home Logic UK Ltd ('Home Logic') is a provider of home energy saving solutions and products.

Between 1 April 2015 and 31 July 2016, Home Logic made 1,475,969 unsolicited direct marketing calls promoting its services to subscribers. During this period, 136 complaints were made to the TPS regarding these calls by Telephone Preference Service ('TPS') registered individuals. The TPS is a register of numbers allocated to subscribers who have notified the TPS that they do not wish to receive unsolicited calls for direct marketing purposes on those lines.

Home Logic licensed the data used to make the calls from third party data providers. These third parties assured Home Logic that the data subjects had 'opted-in' and/or were screened against the TPS. However, one third party provider made it clear in its contract with Home Logic that it was the purchaser's responsibility to conduct such screenings.

Home Logic informed the ICO that it did upload data to a dialler system for screening against the TPS. However, due to technical difficulties, the dialler system was unavailable for a period of 90 days during which time Home Logic continued to make unsolicited direct marketing calls without taking any other steps to screen against the TPS.

Home Logic was unable to provide evidence that it had consent to make calls to the subscribers who had complained to the TPS.

ICO finding

The ICO held that Home Logic made unsolicited direct marketing calls to subscribers who had registered with the TPS without obtaining prior consent (Regulation 21 of PECR).

Although the ICO determined that Home Logic did not deliberately contravene Regulation 21 of PECR, it ought reasonably to have known that there was a risk that these contraventions would occur, particularly because:

- Home Logic relied heavily on direct marketing due to the nature of its business;
- the issue of unsolicited calls was widely publicised by the media as being a problem;
- the dialler system used by Home Logic to screen against the TPS was unavailable for 90 days during which time Home Logic continued to make unsolicited calls without taking any steps to screen against the TPS; and
- the ICO had published detailed guidance for companies carrying out marketing explaining the legal requirements under PECR.

The ICO further held that Home Logic did not take reasonable steps to prevent the contravention, which could have included the following:

- asking its third party data providers for evidence that subscribers had consented to receiving calls; and
- screening the data against the TPS itself, regardless of any assurances that might have been given by the third party data providers.

Harm

The ICO was satisfied that the contravention was 'serious' as there had been multiple breaches of Regulation 21 of PECR over a 15 month period, leading to a significant number of complaints being made. However, it did not appear that any individuals affected suffered financial damage.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Types of breach per legislation

PECR breaches: **30**

Data Protection Act (DPA) breaches: **24**



24 August 2017

£70,000

DPA – 7th Principle

Factual background

In July 2011, the Council's digital team launched its 'Home Care Allocation System' ('HCAS'). Third party home care providers could access HCAS to confirm that they had capacity to support a particular service user. The home care providers were each sent a link to HCAS via e-mail. There were no access controls on HCAS, such as the use of a username or password.

On 14 June 2016, a member of the public informed Nottinghamshire that HCAS could also be accessed via an internet search engine. They were concerned that, 'Should someone who would wish to prey on a vulnerable person...it would not be difficult for them to attend one of the streets listed, find where the carers attend and subsequently consider attempting a burglary or similar knowing the service user is very likely to be vulnerable or elderly.'

At that time, HCAS contained a directory of 81 service users including their gender, addresses (to the extent required by each home care provider) and post codes; personal care needs and care package requirements such as the number of home visits per day and whether the service user was currently in hospital. This personal data would allow a motivated individual to identify a service user.

ICO finding

The ICO found that the Council did not have appropriate technical and organisational measures in place for ensuring so far as possible that such an incident would not occur (DPA – 7th Principle). In particular, the ICO found that HCAS did not have in place an authentication process which identified a user before allowing them access to the system, such as a username or password.

The ICO did not consider the contravention deliberate. However, the Council should have known or ought reasonably to have known there was a risk that unauthorised or unlawful access would occur unless it ensured the personal data held on HCAS was appropriately protected. The ICO found that the Council had failed to take reasonable steps to prevent the contravention.

Harm

The ICO was satisfied that the contravention identified was 'serious' due to the number of data subjects, the nature of the personal data held on HCAS and the potential consequences of unauthorised or unlawful access.

The ICO held that the contravention was likely to cause distress to the service users if they knew that their personal data had been accessed by unauthorised individuals over a five year period, and that such distress was likely to be substantial because the nature of data, number of service users, and the vulnerable nature of service users. The ICO also found that service users would be distressed simply through having justifiable concerns that their information has been further disseminated, even if those concerns do not actually materialise.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- HCAS was taken offline on 14 June 2016.
- Nottinghamshire reported this incident to the Commissioner and was co-operative during her investigation.
- A monetary penalty might have a significant impact on the Nottinghamshire's reputation, and to an extent, its resources.

6 September 2017

£85,000

PECR – Regulation 21, Regulation 24

Factual background

True Telecom Limited ('True Telecom') provides telephone services to businesses and residential consumers. Services include broadband, line rental, calls, and mobile sim-only plans.

Between 6 April 2015 and 27 April 2017, the ICO received 201 complaints through the Telephone Preference Service ('TPS') about unsolicited direct marketing calls made by True Telecom. The TPS is a register of numbers allocated to subscribers who have notified them that they do not wish to receive unsolicited calls for direct marketing purposes on those lines. All of these complaints were made by individual subscribers who were registered with the TPS.

Some of the complainants reported that they received unsolicited calls from a withheld number and that the calls were misleading because the callers gave the impression that they were calling from BT Openreach.

On 18 May 2016, the ICO informed True Telecom of the complaints received. True Telecom's response stated that it was unable to provide any consent for the calls and that it had obtained the data used to make the calls through 'data scraping' – during which a software tool is used to pull or 'scrape' information from open source listings into a spreadsheet. Once data is scraped, the number is uploaded to True Telecom's TPS screening software before being allocated to their internal sales team.

Although the TPS screening software was used, True Telecom advised that a selection of data was made available to the outbound sales team. This data was not subject to TPS screening during a transitional period after the departure of the previous IT manager.

ICO finding

The ICO held that True Telecom made unsolicited direct marketing calls to subscribers whose numbers were registered with the TPS without prior consent (Regulation 21 of PECR).

The ICO was also satisfied that, for the purposes of Regulation 21 of PECR, the 201 complaints were made by subscribers who had registered with the TPS at least 28 days prior to receiving the calls and had not given prior consent to True Telecom to receive calls.

True Telecom was unable to establish that subscribers had consented to be called due to the nature of the way it had obtained the data. ICO guidance on direct marketing explains that organisations must keep clear records of what an individual has consented to and when and how this consent was obtained.

In addition, the ICO held that True Telecom knew or ought reasonably to have known that there was a risk that these contraventions would occur given that True Telecom relied on direct marketing due to:

- the nature of its business;
- the way in which it sourced its data; and
- the fact that the issue of unsolicited calls was widely publicised by the media as being a problem.

The ICO also held that True Telecom failed to take reasonable steps to prevent the contraventions, which could have included:

- carrying out adequate screening of the data against the TPS register;
- ensuring that the entire TPS file they received from their provider was uploaded on their system before making calls; and
- providing telesales staff with written procedures and training regarding the requirements of PECR and how to comply with them.

Harm

The ICO was satisfied that the contravention was 'serious', owing to the number of individuals affected, and True Telecom's grievous failure to screen the telephone numbers against the TPS. In addition, the contraventions took place over a period of approximately two years. The ICO also noted that it was reasonable to suppose that considerably more calls were made, and those affected had not complained.

Aggravating factors

- True Telecom had previously been contacted by the ICO regarding complaints and received guidance related to this.
- Despite being advised by the ICO of the requirement to do so, True Telecom failed to register as a data controller under the Data Protection Act 1998 and was prosecuted for this offence in March 2017. The ICO considered this indicative of True Telecom's attitude towards compliance with regulatory requirements.
- The ICO also took account of the fact that True Telecom had failed to identify the person who was making the calls, or provide contact details on which the person could be reached free of charge.

Mitigating factors

- There is potential for damage to True Telecom's reputation which may affect future business.

6 September 2017

£45,000

PECR – Regulation 22

Factual background

Cab Guru Limited ('Cab Guru') is the company behind the mobile application called 'Cab Guru', which allows customers to compare taxi and min cab fares and pickup times and then to book the selected service.

Cab Guru marketed this service by sending direct marketing text messages, inviting customers to download the application.

Between 27 May 2016 and 5 June 2016:

- 360,373 unsolicited text messages were delivered;
- 165 complaints were made via GSMA's Spam Reporting Service (the data from which the ICO is provided access to); and
- One complaint was made to the ICO.

On 25 June 2016 the ICO wrote to Cab Guru requesting evidence of consent relied upon to send the text messages. Cab Guru stated that it had undertaken a one-day SMS marketing campaign targeted at customers, whose telephone numbers had been obtained from Cab Guru's associated taxi companies. Cab Guru did not obtain consent directly from the SMS recipient, however the associated taxi companies had asked customers for their consent to receive text messages.

The ICO subsequently requested copies of the customer agreements to evidence the consent relied upon. Cab Guru confirmed that there were no formal written contract/consent as the text message contact was requested by the customer via the online web booking form or mobile phone apps.

Upon further investigation, the ICO discovered that the associated cab companies incorporated an automatic agreement to marketing in privacy policies or terms & conditions for use of their services. The consent to the marketing was therefore a compulsory term rather than a discretionary one.

ICO finding

The ICO found that Cab Guru successfully sent 360,373 unsolicited direct marketing text messages without the appropriate consent (Regulation 22 of PECR). Another further 346,277 had failed to send.

The ICO held that this contravention was not deliberate. However, Cab Guru knew or ought to have known that there was a risk that these contraventions would occur given that the issue of unsolicited text messages has been widely publicised by the media, and that the ICO had published detailed guidance in this area. Cab Guru had therefore been negligent in sending the text messages.

Further, the ICO found that Cab Guru failed to take reasonable steps to prevent the contravention. In particular, it failed to:

- put in place appropriate systems and procedures to ensure that it had the specific consent of those whom it had sent marketing text messages; and
- adequately record the source of the data used or retain evidence of any consent obtained.

Harm

The ICO was satisfied that the contravention caused distress among consumers, as evidenced by the large number of complaints made. Furthermore, the ICO determined that the contravention was 'serious' given the high number of contraventions, and the fact that this number could have been much larger, as 346,277 messages had failed to send.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Your Money Rights Ltd

11 September 2017

£350,000

PECR – Regulation 19

Factual background

Your Money Rights Ltd ('YMR') is a payment protection insurance ('PPI') company.

Between 8 March 2016 and 27 July 2016, YMR made 146,020,773 unsolicited automated direct marketing calls concerning PPI claims. During the same period, the ICO received 255 complaints regarding the calls made by YMR.

Upon investigation, it was confirmed that:

- YMR were not identified as the maker of the calls;
- Data was licensed to YMR from third party providers; and
- YMR contracted with a separate third party to make the calls on behalf of YMR.

YMR was unable to provide evidence that it had obtained the necessary consent of the individuals to whom it made the calls to.

ICO finding

The ICO found that YMR made 146,020,773 automated direct marketing calls to individuals without their necessary prior consent (Regulation 19 of PECR).

The ICO stated that it had published detailed guidance for companies carrying out marketing activities explaining their legal obligations under PECR. In particular, it stated that marketing material can only be transmitted via an automated system with the prior consent of the individual.

The ICO held that whilst YMR may not have deliberately set out to contravene PECR, it did deliberately send automated marketing calls on a massive scale to individuals in contravention of Regulation 19 of PECR.

Harm

The ICO was satisfied that the contravention was 'serious' given that YMR instigated the making of over 146 million automated marketing calls to individuals without their prior consent, resulting in 255 complaints being made to the ICO.

While it does not appear that financial loss was suffered by the individuals affected, some may have suffered distress as a result of the provision of their personal data to a third party, or suffered a diversion of resources due to the need to make complaints and deal with the contravention.

Aggravating factors

- YMR may have obtained a commercial advantage over its competitors by generating leads from unlawful marketing practices.
- YMR were not identified as the body instigating the calls and there were no contact details provided by which YMR could be reached free of charge. This contravened regulation 24 of PECR.

Mitigating factors

- There were no mitigating factors.

Easyleads Limited

14 September 2017

£260,000

PECR – Regulations 19 and 24

Factual background

Easyleads Limited ('Easyleads') is a marketing firm based in Coventry.

Between 22 October 2015 and 30 June 2017, Easyleads made 16,730,340 marketing calls to subscribers without their prior consent, resulting in 551 complaints to the ICO.

The automated calls contained recorded messages from Easyleads regarding an entitlement to a grant to replace oil or LPG boilers 'totally free of charge'.

Many of the complaints reported that multiple calls were received and that there was an inability to opt-out of the calls. Others expressed distress as individuals would be expecting urgent calls only to receive an automated message about replacement boilers. Calls were also being made late at night and in the early hours of the morning with particular frequency over the May 2017 bank holiday weekend.

Easyleads was unable to provide evidence that it had the consent of the individuals to carry out such marketing calls.

ICO finding

The ICO was satisfied that Easyleads did not have the consent of the individuals to whom it had made 16,730,340 automated direct marketing calls (Regulation 19 of PECR). The ICO also found that Easyleads failed to include the company name, address and telephone number in their automated messages, pursuant to the requirements of Regulation 24 of PECR.

In particular, the ICO highlighted the following:

- The wording of some of the automated calls was misleading in that it referred to a 'government scheme' and the offer of a 'free boiler'.
- Whilst the automated calls offered an 'opt-out' option, there is evidence to suggest that repeat calls were made to subscribers regardless of this.
- There was a failure to ensure that an effective suppression system was in place to prevent repeat calls to those who had opted out.

The Commissioner is satisfied that Easyleads Limited did deliberately contravene Regulation 19 of PECR in that its actions which constituted the contravention were deliberate.

Harm

The ICO was satisfied that the contravention was 'serious' due to the sheer extent of the contravention: Easyleads made over 16 million automated marketing calls without the prior consent of the affected individuals. This resulted in 551 complaints being made to the ICO. In particular, complainants expressed distress as some would be expecting urgent calls only to receive an automated message about replacement boilers. However, no financial loss is noted.

Aggravating factors

- Within 9 days of receiving a letter from the ICO to confirm that it was under investigation, Easyleads carried out a further marketing campaign and continued to make automated marketing calls.
- The ICO's direct marketing monthly threat assessments showed that one of the CLL's used by Easyleads was the most complained about number for automated calls for four consecutive months, from March 2017 to June 2017.
- Easyleads failed to engage with the ICO in assisting with its investigations, and have failed to respond to queries.

Mitigating factors

- There were no mitigating features.

Xerpla Limited

4 October 2017

£50,000

PECR – Regulation 22

Factual background

Xerpla Limited ('Xerpla') offers design, advertising and marketing services.

Between 6 April 2015 and 20 January 2017 Xerpla transmitted 1,257,580 unsolicited direct marketing emails. These emails promoted products and services of a wide range of third parties, including providers of pet products, wine, motoring services, financial services and boilers.

The emails were sent to individuals who had subscribed to two websites operated by Xerpla – YouSave.co.uk and HeadsYouWin.co.uk. When subscribing, individuals were informed that by submitting their details, they consented to receive newsletters and offers from and on behalf of offer partners and from other similar third party online discount and deal providers. By subscribing, individuals were also consenting to the processing of their information as outlined in a separate Privacy Policy.

In 2016, the ICO received 14 complaints about the receipt of unsolicited direct marketing emails from the two websites through Xerpla.

ICO finding

The ICO held that the consent relied on by Xerpla was not sufficiently informed and therefore did not amount to valid consent (Regulation 22 of PECR).

The ICO held that Xerpla did not deliberately seek to contravene Regulation 22 of PECR but ought to have known that there was a risk that these contraventions would occur. This is particularly the case given that direct marketing of this nature is widely publicised by the media as being a problem and that the ICO has published detailed guidance for organisations explaining their legal obligations under PECR.

The ICO was also satisfied that Xerpla failed to take reasonable steps to prevent the contravention. Reasonable steps in these circumstances could have included seeking appropriate guidance on the rules in relation to electronic direct marketing and ensuring that the consent Xerpla sought to rely on was valid.

Harm

The ICO was satisfied that the contravention was 'serious' due to the large number of data subjects affected by the 1,257,580 emails sent by Xerpla. It is not clear that the contravention caused any financial loss to those affected, however due to the persistent nature of the emails, the contravention may have caused distress or diversion of time in reporting the contraventions.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

Types of breach per legislation

Breach of DPA Principle 1: **2**

Breach of DPA Principle 1 & 2: **10**

Breach of DPA Principle 7: **11**

Breach of DPA Principle 7 & 8: **1**

Breach of PECR 19: **2**

Breach of PECR 19 & 24: **4**

Breach of PECR 21: **7**

Breach of PECR 21 & 24: **1**

Breach of PECR 22: **16**



Vanquis Bank Limited

4 October 2017

£75,000

PECR – Regulation 22

Factual background

Between 9 April 2015 and 16 February 2016, Vanquis Bank Limited ('VBL') instigated a campaign to send 870,849 direct marketing text messages to subscribers. VBL obtained the personal data from third parties and relied on indirect consent for sending the direct marketing text messages sent to subscribers.

VBL came to the attention of the ICO in December 2015 on review of the ICO's 'monthly threat assessment'. This revealed that 15 complaints about VBL had been made to GSMA's Spam Reporting Service, which allows mobile users to report the receipt of unsolicited marketing text messages to the GSMA (the GSMA makes such complaints data available to the ICO). The Commissioner subsequently launched an investigation to determine whether VBL's text message marketing had been carried out in compliance with Regulation 22 of PECR.

Further, between 17 December 2015 and 3 August 2016 620,000 direct marketing e-mails were sent to subscribers by one of VBL's sub-affiliates on behalf of VBL. The ICO received 9 complaints in respect of such e-mails. The indirect consent VBL had relied upon for 7 of the 9 complaints had been obtained through various affiliates and sub-affiliates.

ICO finding

The ICO found that VBL it did not have the appropriate consent of the data subjects to direct marketing text messages or emails (Regulation 22 of PECR).

VBL was unable to evidence that individuals to whom direct marketing text messages and e-mails had been sent had consented to receipt of the messages.

The ICO considered that VBL did not deliberately contravene Regulation 22 of PECR, however, VBL knew or ought to reasonably have known that there was a risk that these contraventions would occur. The ICO also found that VBL failed to take reasonable steps to prevent the contraventions.

Harm

The Commissioner was satisfied that the contravention was 'serious' because in a ten month period VBL sent a total of 870,849 direct marketing text messages to subscribers without their consent. This resulted in 131 complaints being made.

Further, in a five month period VBL instigated the sending of a total of 620,000 direct marketing emails to promote VBL services to subscribers without their consent. This resulted in 9 complaints being made.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

The Lead Experts Limited

10 October 2017

£70,000

PECR – Regulations 19 and 24

Factual background

The Lead Experts Limited ('TLEL') is a marketing firm based in Liverpool.

On 31 October 2016 the Commissioner served a third party information notice on DXI Limited ('DXI') in relation to automated calls made via the DXI voice broadcasting platform from numbers prefixed with 08454290 and 0844337, those being the prefixes for the reported complaint numbers.

DXI responded providing a spreadsheet containing a list of automated calling campaigns instigated by their customers, using these numbers as presentation CLIs ('Calling Line Identifications').

The spreadsheet included the company names, CLIs used, dates of the campaigns and volume of calls made. The information provided showed that, between 4 May 2016 and 5 May 2016, TLEL made a total of 115,341 automated calls.

TLEL denied ever using automatic dialling and stated that its 'only experience with DXI was that of buying a small batch of test leads of which we [TLEL] only dialled a small amount due to the quality not being very good.' DXI, however, provided sufficient evidence to refute this claim including, a signed order form outlining charges for calls to landlines and mobiles, audio files containing voice recordings of the messages to be played when the calls connected, and copies of e-mails in which TLEL supplied DXI with numbers to be loaded onto a dialler as part of their marketing campaign.

TLEL was unable to provide evidence that it had the consent of the individuals to whom it had instigated the transmission of the automated direct marketing calls.

ICO finding

The ICO found that between 4 May 2016 and 5 May 2016 TLEL instigated the transmission of 115,341 automated marketing calls to subscribers (111,072 of which were successful) without their prior consent (Regulations 19 and 24 of PECR).

Furthermore, they failed to include the company name, address and telephone number in their automated messages pursuant to the requirements of Regulation 24.

The ICO was satisfied that TLEL deliberately contravened Regulation 19 of PECR in the sense that TLEL's actions were deliberate.

Harm

The Commissioner was satisfied that the contravention identified above was 'serious' because TLEL instigated the making of 115,341 automated marketing calls to subscribers without their prior consent.

Verso Group (UK) Limited

17 October 2017

£80,000

DPA – 1st Principle

Factual background

Verso Group (UK) Limited ('Verso') is a data broking company.

Whilst investigating two organisations for sending of direct marketing communications in contravention of PECR, it came to the Commissioner's attention that Verso had supplied those companies with large volumes of personal data which was then used in contravention of PECR. Consequently, on 17 March 2016 the Commissioner commenced an investigation into whether or not Verso had obtained and/or supplied the personal data in compliance with Data Protection Principle 1. The Commissioner corresponded extensively with Verso between March and November 2016.

In that correspondence Verso explained how it obtained and supplied personal data, including information about specific transactions. It provided the Commissioner with information about the companies and websites from which it obtained personal data. Verso also provided the Commissioner with evidence of its due diligence measures in respect of companies that had supplied it with personal data. Verso also supplied information about telemarketing campaigns through which it obtained personal data and the scripts for those telephone calls.

The Commissioner considered the terms and conditions and privacy notices applicable to the personal data and found that the data subjects had not consented to their personal data being supplied to Verso and/or for onward sale to other companies for direct marketing purposes. The Commissioner also considered an adjudication of the Direct Marketing Commission (DMC) published in August 2016 concerning Verso's supply of data of over 2 million customer records to be used for an SMS marketing company by a gambling company. In their adjudication the DMC found that Verso had contravened a number of provisions of the Direct Marketing Association's Code.

ICO finding

The ICO found that across the various transactions it reviewed Verso:

- failed to provide the data subjects with sufficiently clear information about the companies to whom their personal data would be disclosed to for direct marketing purposes; and
- sold personal data which it had obtained unfairly, and so the onward sale was also unfair.

The ICO found that these transactions contravened Data Protection Principle 1.

The Commissioner considered that these contraventions were deliberate, in the sense that Verso's actions were deliberate and systemic. Alternatively, Verso knew or ought reasonably to have known that there was a risk that these contraventions would occur and be of a kind likely to cause damage or substantial distress.

Aggravating factors

- TLEL had repeatedly denied all wrongdoing and pleaded ignorance as to the contravention, despite evidence to verify its instigation of the direct marketing. TLEL has also disengaged with the Commissioner during the latter part of the investigation.
- While the CLIs used for the marketing calls were legitimate, they did not identify the company making the call. The CLIs were routed through Buenos Aires making it difficult to trace the company.
- The CLIs were also 'added value' numbers which charged the individual when they would call to try to identify the company.
- The Commissioner also took into account the fact that TLEL did not identify the person/organisation who was instigating the call, or provide details on which the person making the calls could be contacted free of charge.
- When challenged regarding its practice TLEL sought to liquidate the company on 27 July 2017. This was placed on hold pending the Commissioner's investigation.

Mitigating factors

- There were no mitigating features.

Total value of MPNs issued per legislative breach



Breach of DPA Principle 1: **£100,000**

Breach of DPA Principle 1 & 2: **£120,000**

Breach of DPA Principle 7: **£966,000**

Breach of DPA Principle 7 & 8: **£200,000**

Breach of PECR 19: **£750,000**

Breach of PECR 19 & 24: **£618,000**

Breach of PECR 21: **£420,000**

Breach of PECR 21 & 24: **£85,000**

Breach of PECR 22: **£948,500**

16 November 2017

£45,000

PECR – Regulation 22

Factual background

Hamilton Digital Solutions Ltd ('HDSL') is a London based online technology and telecoms company.

Between 1 April 2016 and 19 September 2016, HDSL used a public electronic telecommunications service to transmit 156,250 unsolicited communications by e-mail to individual subscribers for the purposes of direct marketing.

HDSL used third-parties to send the marketing text messages, who would act as an 'introducer' of customers to HDSL. In response to correspondence from the ICO, HDSL indicated that they would carry out an 'extensive due diligence exercise' with each new introducer, including a review of the permissions held; its 'privacy policy'; consents; and data sources.

HDSL gave the ICO details of the consent relied upon for the direct marketing that had been provided by the 'introducer' which sent the messages.

ICO finding

The ICO found that HDSL instigated the sending of 156,250 unsolicited direct marketing text messages without consent (Regulation 22 of PECR).

In particular, the ICO stated that organisations can generally only send marketing texts to individuals if that person has specifically consented to receiving them from the sender. The ICO also explained that particular care must be taken when relying on 'indirect consent', and that it is not acceptable to rely on assurances given by third party suppliers without undertaking proper due diligence. The ICO found the evidence of consent relied upon by HDSL for the direct marketing that had been provided by the 'introducer' was insufficient for the purposes of Regulation 22 PECR.

The ICO did not consider the contravention deliberate but stated that HDSL should have known or ought reasonably to have known that there was a risk that this contravention would occur. The ICO found that HDSL had failed to take reasonable steps to prevent the contravention.

Harm

The ICO was satisfied that the contravention identified was 'serious', owing to the fact that between dates of 1 April 2016 and 19 September 2016, HDSL sent a total of 156,250 direct marketing text messages to subscribers without their consent. Between the periods of 1 April 2016 and 9 May 2016, this action resulted in 595 complaints.

Aggravating factors

- No mention of aggravating features.

Mitigating factors

- There were no mitigating features.

The Commissioner further considers that Verso failed to take reasonable steps to prevent such a contravention, in that:

- Verso failed to undertake adequate due diligence when selecting its data suppliers in order to ensure that it received and used personal data fairly;
- Verso failed to incorporate adequate contractual terms requiring its data suppliers to ensure that personal data was obtained and provided to Verso fairly;
- Verso failed to take practical steps to satisfy itself that data subjects were provided with sufficiently specific information to help them understand what would be done with their personal data; and
- when obtaining personal data from data subjects, Verso should have provided sufficiently specific information about the companies to whom Verso would provide personal data.

Harm

The Commissioner considers that these contraventions were serious, in that:

- they involved large volumes of personal data and large numbers of data subjects;
- Verso's contraventions were systemic: they were not isolated, one-off or occasional errors; and
- there were numerous contraventions extending over a period of years.

Aggravating factors

- Verso's contraventions were numerous, systemic and serious. They took place over a number of years and affected many thousands of data subjects.
- Verso was unhelpful and obstructive during the Commissioner's investigation. It failed to provide some requested information, obfuscated in many of its answers and declined to co-operate adequately on a number of occasions. The Commissioner had to threaten to issue formal information notices in order to obtain answers to some of her questions.
- Verso was unable to demonstrate how it had taken steps to ensure compliance with the DPA.
- In the circumstances, the Commissioner considers Verso to have acted in disregard of its legal obligations.

Mitigating factors

- Verso provided the Commissioner with some relevant information about its practices during the course of her investigation.
- The penalty could have a significant reputational impact on Verso.



UK Prosecutions

Of those who commit criminal
offences under the Act
through the Court system

Total

11

True Telecom Ltd

15 March 2017

True Telecom Limited has been prosecuted at Medway Magistrates Court for the offence of processing personal data without having an entry in the register maintained by the Information Commissioner.

Action:

The telecommunications company was found guilty of the offence under section 17 of the Data Protection Act 1998, and was fined £400, ordered to pay costs of £593.75 and a victim surcharge of £40.

Sally Anne Day

16 May 2017

A former administration employee of Crickhowell Group Practice, part of the Powys Health Trust Board was prosecuted at Newport Crown Court for repeatedly accessing the sensitive medical records of two patients without the consent of the data controller.

Action:

Ms Sally Anne Day pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £400, ordered to pay costs of £350 and a victim surcharge of £40.

Joseph Walker

8 June 2017

Following a prosecution by the ICO, Joseph Walker pleaded guilty to section 55 Data Protection Act offences before Liverpool Magistrates' Court. The offence related to making blagging calls to obtain information about policy holders and the road traffic accidents they had been involved in, from insurance companies. At the time of the offences the defendant had worked at a claims management company, UK Claims Organisation Ltd, based in Liverpool, together with co-defendants Lesley Severs and Kayleigh Billington, who were sentenced last year. It was the prosecution case that data originally obtained unlawfully from a car hire company was used by the employees of the claims management company as leads, to make blagging calls to insurance companies. In the calls the defendants used various guises and tried to obtain further information from the insurers, in order to be able to sell cases on to solicitors as personal injury claims.

Action:

Joseph Walker pleaded guilty to 12 offences under section 55 of the Data Protection Act 1998 and 44 like offences were taken into consideration, for which he was fined £2,000, ordered to pay a victim surcharge of £15 and prosecution costs of £1,600.

Stuart Franklin

21 July 2017

Stuart Franklin has been prosecuted at Birmingham Magistrates' Court for the offence of unlawfully disclosing personal data. The defendant, who at the time worked at a Walsall based domestic services company, emailed the CVs of 26 job applicants to a third party company without his employer or the data controller's consent.

Action:

Mr Franklin pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £573, ordered to pay £364 prosecution costs and a £57 victim surcharge.

Brioney Woolfe

11 August 2017

A former employee of Colchester Hospital University NHS Foundation Trust, Brioney Woolfe was prosecuted at the Colchester Magistrates' Court. Woolfe accessed the medical records of several people without a business purpose to do so while employed as a health care assistant by Colchester Hospital University NHS Foundation Trust.

Action:

Woolfe pleaded guilty to two offences under section 55 of the Data Protection Act for accessing the sensitive health records of friends and people she knew and disclosing some of the personal information obtained.

Ms Woolfe was fined £400 for the offence of obtaining personal data and £650 for disclosing it. Ms Woolfe was ordered to pay prosecution costs of £600 and a victim surcharge £65.

Linda Reeves

4 September 2017

A former data co-ordinator employed by The University Hospitals of North Midlands NHS Trust has been prosecuted at North Staffordshire Magistrates' Court. Linda Reeves accessed the sensitive medical records of colleagues as well as people she knew that lived in her locality, without the consent of the data controller.

Action:

Ms Reeves pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £700, ordered to pay costs of £364.08 and a £70 Victim Surcharge.

Nilesh Morar

21 September 2017

Nilesh Morar has been prosecuted at Nuneaton Magistrates' Court for the offence of unlawfully obtaining personal data. The defendant, who at the time worked at Leicester City Council, emailed personal data relating to 349 individuals, which included sensitive personal data of service users of the Adult Social Care Department, to his personal email address without his employer or the data controller's consent.

Action:

Mr Morar pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £160, ordered to pay £364.08 prosecution costs and a £20 victim surcharge.

Nicola Wren

16 October 2017

A former administrator employed by Kent and Medway NHS and Social Care Partnership Trust has been prosecuted by the ICO at Medway Magistrates' Court.

Nicola Wren accessed the sensitive medical records of a patient who was known to her 279 times in a three week period, without any business need to do so, which was without the consent of the data controller.

Action:

Ms Wren pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £300, ordered to pay costs of £364.08 and a £30 Victim Surcharge.

Robert Morrissey

9 November 2017

A former employee of a community based counselling charity has been prosecuted by the ICO at Preston Crown Court. Robert Morrissey sent spreadsheets containing the information of vulnerable clients to his personal email address without any business need to do so, which was without the consent of the data controller.

Eleven emails were sent from his work email account on 22 February 2017, which contained the sensitive personal data of 183 people, three of whom were children. The personal data included full names, dates of birth, telephone numbers and medical information. Further investigation showed that he had sent a similar database to his personal account on 14 June 2016.

Action:

Mr Morrissey pleaded guilty to three offences under section 55 of the Data Protection Act and was sentenced to a two year Conditional Discharge, ordered to pay costs of £1,845.25 and a £15 Victim Surcharge.

Clair Francis

9 November 2017

Clair Francis, who worked as a Coding Officer for Dudley Group NHS Trust, pleaded guilty to one offence of obtaining personal data and one offence of disclosing personal data. She accessed her neighbour and former friend's medical records and disclosed information about a baby.

Action:

Ms Francis was fined £125 for each offence and ordered to pay costs of £500 and a victim surcharge of £30.

Marian Waddell

13 November 2017

Marian Waddell, a former nursing auxiliary was fined for accessing a patient and her neighbour's medical records without a valid legal reason. She worked at Royal Gwent Hospital in Newport and unlawfully accessed the records of a patient who was also her neighbour.

Action:

She was fined £232 and was ordered to pay £150 costs and a victim surcharge of £30.

10 out of 11

prosecutions were due to
unlawfully obtaining or
disclosing personal data



Total number of prosecutions per year

2017: **11**

2016: **16**

2015: **11**

2014: **18**

2013: **7**

2012: **6**





Attend our Data Protection Bootcamps

Join our Data Protection Bootcamps every month by WebEx or in person.

They provide:

- Accessible insights into the practicalities of operating in a GDPR-live environment
- Pragmatic recommendations on how to operationalise Data Protection law and reduce operational, legal and commercial risk
- Learning and networking opportunities with your peers

We also offer tailored in-house Data Protection training and awareness sessions.

For further information please contact us at DP_Bootcamps@uk.pwc.com



UK Undertakings

Commit an organisation to a particular course of action in order to improve its compliance

<i>Total</i>	<i>11</i>
Private Sector	<i>1</i>
Public Sector	<i>10</i>

6 January 2017 (follow up to Undertaking issued 19 April 2016)

DPA – 1st Principle

On 16 December 2016 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by NHS Digital (formerly known as HSCIC) in relation to the undertaking it signed on 19 April 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

NHS Digital agreed to the undertaking following the Commissioner's investigation of the way NHS Digital shared patient data for purposes other than direct care. Specifically, that NHS Digital was not able to collect, record or implement Type 2 objections registered by patients with their GPs, for legal and technical reasons, which resulted in Type 2 objections not being implemented for approximately 700,000 patients. Further, the HSCIC had not taken steps to inform affected patients other than a statement placed on its website (DPA – 1st Principle).

The review demonstrated that NHS Digital has taken appropriate steps and put plans in place to address the requirements of the undertaking and to mitigate the risks highlighted. NHS Digital confirmed that it has taken the following steps:

1. HSCIC should establish and operate a system to process and uphold Type 2 objections, in accordance with the Direction from the Secretary of State.

- NHS Digital has established and currently operates a system to process and uphold Type 2 objections. This was done by directing GPs to supply the necessary data via the General Practice Extraction Service or HSCIC Secure Electronic File Transfer system. Internal technological systems have been developed to receive, record and manage these patient objections around a central Patient Objections System. Organisational processes have been developed for NHS Digital staff to be aware of, and correctly use, the Central Patient Objections System where their work makes this necessary. Auditable information is recorded for these processes and the policies are due for regular review. Specific roles, (such as Information Asset Owners,) have been identified as responsible for aspects of the system and such individuals have received appropriate guidance. A steering group and system user group have been established as part of ongoing monitoring to ensure continued compliance.

2. HSCIC should ensure measures are put in place so that any patients who have previously registered a Type 2 objection, or patients who register a Type 2 objection in future, are provided with clear fair processing information that enables them to understand how the Type 2 objection will be applied and how their data will be used.

- NHS Digital has updated the fair processing information on its website to describe and explain Type 1 and Type 2 objections to patients. The NHS Choices website has also been updated to include clear information on objections and contains referral links to more information on the NHS Digital website relating to objections. Additionally, awareness about objections was relayed via the external relations manager to selected external organisations who regularly offer advice to patients who contacted them.

3. HSCIC should contact recipients of data sets it provided in the period January 2014 – April 2016 (where Type 2 objections can be processed and upheld in accordance with the Direction) and make them aware that the data sets may include records relating to patients who have chosen to opt out. HSCIC should do this within three months of the undertaking.

- Using its Data Access Release team and Data Release Register NHS Digital was able to identify the recipients of data sets provided between January 2014 and April 2016 that were likely to contain records of patients who had registered a Type 2 objection and not covered by an exemption. A letter was sent on 19 July 2016 (the day after the three months described in the undertaking expired), informing the recipient that the data set may include records as described above. Further contact was made if a recipient did not confirm receipt of the original correspondence. This was done by letter or telephone as appropriate. As of 19 October 2016 it was reported that all recipients had been successfully contacted.

4. HSCIC should contact recipients of data sets it provided in the period January 2014 – April 2016 (which included patient data where Type 2 objections can be processed and upheld in accordance with the Direction) and where the agreement allowed the recipient to onwardly disseminate the data, to make them aware that this data should no longer be disseminated further. HSCIC should do this within three months of the undertaking.

- It was identified that four data sharing agreements included provision to onwardly disseminate data. The circumstances of each were examined in detail and found that for each, for different reasons, no action was required in relation to the undertaking requirement

5. **HSCIC should contact recipients of data sets it provided in the period January 2014 – April 2016 (which included patient data where Type 2 objections can be processed and upheld in accordance with the Direction) to inform them that, where possible, the data sets should be destroyed or deleted and replaced with a new data set, which reflects patient opt outs, provided by HSCIC in its place. Whether it is possible to destroy or delete the data will depend on whether or not it has already been processed and used, such as in a research study or as part of business intelligence information made available to a Trust. HSCIC will collect and retain a certificate of destruction where it is possible for data to be destroyed or deleted.**
 - As part of contacting the recipients of the relevant data sets as previously mentioned, NHS Digital advised that where possible the data sets should be destroyed/deleted. A log of destruction certificates has been kept where they have been provided to NHS Digital and requests for replacement data sets are being processed if appropriate.
6. **HSCIC should revisit the matter of objections following the completion of the National Data Guardian review and consider whether its systems and processes can be modified to allow the Type 2 objection to be applied in circumstances where this is not currently possible.**
 - NHS Digital has stated that they have examined the National Data Guardian's (NDG) review of data security, consent and opt-outs published 6 July 2016. NHS Digital reports that for the systems identified where it is currently accepted as not possible to apply the Type 2 objections the review does not change this situation. The NDG review does not recommend any changes to existing arrangements pending a full consultation on the proposed new consent/opt-out model. NHS Digital has undertaken that the systems identified will be examined again following the publication of the response by the Secretary of State to the NDG review, as there may be proposals made regarding legislative changes that impact the situation.
7. **HSCIC should ensure measures are put in place so that any patients affected by this incident can be made aware that it is possible that their personal data has been shared with third parties against their wishes. This process should be completed within six months.**
 - NHS Digital has, as well as relying on the press coverage regarding the incident to raise awareness, published relevant information to the NHS Choices website on the right to opt-out of identifying information of patients being shared beyond their GP practice or NHS Digital. It has produced standard wording that was sent to all GP practices asking for the information be made available to patients. It also provided the same to both Healthwatch England and the Patients Association and requested they disseminate it throughout their organisations to aid in informing patients.
 - However, the requirement to make patient's affected by the incident aware that their personal information has been shared with third parties against their wishes has not been fulfilled. The wording used on the NHS Choices website is 'The HSCIC has started to uphold type 2 objections from 29 April 2016'. It does not make clear that there was sharing carried out prior to the date where objections made were not being honoured. There is an assumption that while mentioning that sharing occurs, and the objections will be honoured from 29 April 2016, the reader will know that prior to this date even though they had objected, that objection was not honoured and sharing took place. It must be considered if it is a reasonable assumption that the average individual would know that the delay caused inappropriate sharing. While correspondence to GPs and third party organisations is more detailed, there is no evidence that any did pass on the information to patients, or that GPs made it available to returning patients who attended their surgeries.

Although NHS Digital took appropriate steps and put plans in place to address some of the requirements of the undertaking, the Commissioner found that further work needed to be completed by 18 April 2017 to fully address the agreed actions. In particular:

NHS Digital should take further action:

- To make it clear by amending published material that type 2 objections received prior to 29 April 2016 were not honoured prior to this date, and so information was shared incorrectly from January 2014.
- To assess the effectiveness of the program of distributing material to GPs and other organisations to raise patient awareness of the failure honour received objections.

Cornwall Council

3 February 2017 (follow-up to Undertaking issued 16 September 2016)

DPA – 7th Principle


On 30 January 2017 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Cornwall Council in relation to the undertaking it signed on 16 September 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

Cornwall Council agreed to the undertaking following the Commissioner's investigation of eight data breaches that occurred over a 2 year period, some of which involved disclosures made in error, which revealed that some staff members had not received data protection training. The Commissioner's investigation also found that the general uptake of data protection training across Cornwall Council was unsatisfactory (DPA – 7th Principle).

The review demonstrated that Cornwall Council has taken appropriate steps to address the three requirements of the undertaking:

1. All current staff members responsible for the handling of personal data should receive appropriate, specific data protection training. This process should be completed within three months.
 - In November 2016 Cornwall Council confirmed within their Uptake of Mandatory Information Governance Training Report that over 83% of Cornwall Council employees had completed their Information Governance training within a two year period. 83% of employees accounted for all of Cornwall Council staff, excluding those who were long term absentees.
2. Such training should be refreshed at regular intervals, not exceeding two years and its provision monitored and recorded.
 - The 'Uptake of Mandatory Information Governance Training Report' states that Cornwall Council monitor compliance with the requirement to complete the Information Governance training at least every two years. Compliance reports are reviewed at the Information Governance steer group and the Corporate Directors' Team on a monthly basis to identify any employees who are due to complete their training so that follow up action can be taken to ensure compliance with the training requirement.
3. New staff members responsible for the handling of personal data are given appropriate, specific data protection training upon induction.
 - Cornwall Council provided copies of their corporate induction checklists, New Employee Checklist and Induction Checklist for Managers Who Manage New Staff – Managers' Induction Checklist for New Staff. The checklists state that it is a mandatory requirement that new employees complete their Information Governance training within their first week of employment.

Total number of undertakings per year



	Public	Private
2017:	10	1
2016:	20	10
2015:	16	17

21 February 2017

DPA – 7th Principle

The Information Commissioner (the ‘Commissioner’) was informed of several similar data protection incidents by Pennine Care NHS Foundation Trust (‘the Trust’) over a twelve month period. The number of incidents reported is of concern especially as they are repeated in nature. The Commissioner also identified delays in reporting with limited information provided, even with ample time to conduct an internal investigation.

One of the incidents occurred in April 2015 and involved a CAMHS patient letter for a GP follow up being sent to a neighbour containing sensitive diagnosis information. On this occasion the envelope was not marked ‘private and confidential’ or for ‘addressee only’. This incident was seen to be representative of subsequent reported data breaches to the Commissioner, where personal information was posted to the wrong person in error.

Information Governance concerns have been raised within the CAMHS service in general, particularly related to an inconsistency with checking patient addresses on internal systems or on correspondence before being sent. There were also identified concerns around addressees on patient records not being kept up to date. During the Commissioner’s investigation into similar security incidents, it was also found that administrative tasks were being undertaken by clinicians who were not clear about the correct administration procedures to protect personal data.

A further data security incident occurring in July 2016 involved a letter being sent to an outdated address containing confidential mental health information and its impact on the committal of an offence. Whilst the confidential letter had been returned to the service, it had been opened by an unintended recipient and could have been accessed further, seeing as this was returned by a third party.

The investigation found that staff failed to check the Electronic Patient Record for the correct address and whilst this can be seen to be attributable to human error, there were concerns around the level of training undertaken by staff. Information Governance training was completed post incident and reliance only placed upon previous experience and college based training.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

1. Procedures are put in place to ensure any reported breach of security relating to personal data is acted upon promptly and any containment and remedial measures are swiftly enforced. The Incident Reporting Policy should include provisions to train staff around reporting to timescales and to provide the most pertinent information to assist an investigation, internal categorisation and prompt remedial measures.
2. The data controller shall ensure all processes within the CAMHS service are standardised across all teams and staff duties between administration staff and clinicians are clearly defined.
3. To review and clarify relevant checking procedures when sending patient correspondence. This is to include procedures around patient record keeping to ensure they are kept up to date. Any related guidance should be disseminated to all staff.
4. The completion of mandatory induction data protection training, in relation to both the requirements of the Act and the data controller’s policies concerning the use of personal data, is appropriately enforced. Completion of such training, including that of regular refresher training, shall be recorded and monitored to ensure compliance.

28 March 2017 (follow-up to Undertaking issued 6 June 2016)

DPA – 7th Principle

During March 2017 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Wolverhampton City Council (WCC) in relation to the undertaking it signed on 2 June 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

WCC agreed to the undertaking following the Commissioner's investigation of an incident that involved an email containing a spreadsheet holding the personal information of employees at 73 educational establishments, being sent in error to an external recipient (DPA – 7th Principle).

The ICO review found that WCC has taken steps and put plans in place to mainly address the requirements of the undertaking as follows:

- A report was submitted to the Council's Strategic Executive Board on 19 July 2016, including a proposed action plan to ensure that the requirements of the ICO undertaking would be met.
- A review of the 'Protecting Information' e-learning module was carried out and the module was updated.
- An email was sent to employees in August 2016 who had not completed or that needed to retake the Protecting Information; eLearn, including a deadline of 30 September 2016 for completion. This was extended to the 30 November 2016 and if any of WCC's employees had not completed it by that point, WCC ensured that they had completed it by the 3 March 2017 in line with the ICO's undertaking requirements.
- Between July 2016 and February 2017, a series of communications were issued across WCC to raise awareness of the ICO undertaking, including the requirement for all WCC employees to complete the Protecting Information e-learning module. These communications included: messages sent via email in the form of 'Core Briefs', email reminders from Organisational Development, messages published on WCC's intranet, managing director briefings, specific internal red banner messages on WCC's intranet and key message reminders at directorate and team meetings.
- Additionally, WCC ran several Information Governance (IG) Surgeries during December 2016 and 15 IG Surgeries across 4 days during February 2017. These IG Surgeries were dedicated to delivering the Protecting Information eLearning training.
- WCC continued to work with their Workforce Development Team and the Learning Pool (providers of the Learning Hub – the Council's e-learning training system), to implement a solution which would enable WCC to track and monitor employees training completion. This was implemented in July 2016.

- The Learning Hub now has a tab which specifies that protecting information e-learning training is mandatory for all employees.
- Between July 2016 and February 2017, regular updates on the completion of the protecting information e-learning training were provided to the Senior Strategic Board – with any follow-up action being undertaken by area directors.
- WCC have confirmed that the Protecting Information e-learning refresher training will now take place every 12 months. WCC employees will receive an automated email reminder when they are due to complete the protecting information e-learning training.
- Between 3 June 2016 and 2 January 2017, 98% of WCC's employees had completed their Protecting Information e-learning 3 refreshing training and 86% of employees had completed their protecting information e-learning induction training.
- Between 3 June 2016 and 3 March 2017, 99% of WCC's employees had completed WCC's mandatory induction and refresher Protecting Information e-learning training.

Although WCC has largely taken appropriate steps to comply with the undertaking, the ICO advised that WCC continue to work in the following areas to further improve their data protection compliance:

- 1. The data controller shall devise and implement a system to ensure that completion of data protection training is monitored and that procedures are in place to ensure that staff who have not completed training within the specified time period do so promptly. This should be completed within three months of the undertaking.**
 - As line managers are responsible for ensuring that their team/s completes any mandatory training, WCC should continue to look at providing managers with an additional dashboard solution that will provide them with information about which staff have completed the Protecting Information e-learning training.
 - WCC should consider producing a training communications plan each year to ensure continuous awareness of the Protecting Information e-learning training and the requirements of the Data Protection Act.
- 2. The data controller shall ensure that all staff handling personal data receive data protection training and that this training is refreshed at regular intervals, not exceeding two years. The data controller should ensure that all staff that handle sensitive personal data regularly, receive refresher training within six months of the date of the undertaking, and all other staff have received refresher training within nine months of the date of the undertaking.**
 - WCC should ensure that they monitor and produce statistical reporting information for the protecting information learning module, specifically in respect of employees that handle sensitive personal information.

3 April 2017 (follow-up to Undertaking issued 19 July 2016)

DPA – 7th Principle

In March 2017 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Northern HSC Trust in relation to the undertaking it signed in July 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

Northern HSC Trust agreed to the undertaking following the Commissioner's investigation of an incident involving 11 emails, which were intended for a doctor's personal non-trust account, being sent to a member of the public with the same name over a two year period (DPA – 7th Principle).

The ICO noted that Northern HSC Trust has taken some steps to meet the requirements of the undertaking; however there are still some areas of concern which need addressing to mitigate the highlighted risks. In particular:

- 1. The data controller must ensure that all staff, including locum doctors, 3rd Party contractors, temporary (agency/bank) staff and volunteers, whose role involves the routine processing of personal and sensitive personal data, undertakes mandatory data protection and data handling induction training and regular refresher training on the requirements of the Act.**
 - All staff at the Trust are now required to do Information Governance (IG) awareness training during their induction. This training will then be refreshed every three years. The most recent compliance report that has been provided, states that 84% of staff have completed the IG Training and 84% of managers have completed the POPI training in December 2016. Although this is an improvement, the Trust still needs to ensure that all staff are completing the IG training within the given time. It has been reported that the IG Training booklet and package for locum doctors and agency staff is still under review. Due to the fact that this has yet to be implemented, there is still a risk that IG incidents will occur due to the lack of training. However the Trust has provided evidence showing that the contractual terms with external domiciliary care providers have been revised. This will reassure the trust the relevant IG training will be given to these contractual staff.
- 2. Provision of such training shall be recorded and monitored with oversight provided at a senior level against agreed Key Performance Indicators (KPI) to ensure completion. In addition, the data controller shall implement follow-up procedures to ensure that staff who have not attended/completed training do so as soon as is practicable.**
 - IG Training KPI and monitoring reports are being produced. These reports should be produced every quarter; evidence of the September report was received but nothing from this year. It has been reported that these reports are provided to all the directorates, the Trust Board and the Corporate Governance Steering Group.

However no evidence has been provided to show that this information is being reported to the Trusts Board. The said reports are also used by management to monitor staff members that have not completed the training in given timeframe. Again there is no evidence showing this. There are also no processes in place to show what the consequences are if staff members repeatedly fail to complete the IG training.

- 3. The data controller shall ensure that staff, including Locum doctors, 3rd party contractors, temporary (agency/bank) staff and volunteers are aware of the content and location of its policies and procedures relating to the processing of personal data, specifically the procedure for reporting and recording IG breaches. If not already in place, a mechanism to ensure that staff are updated of any changes to these policies and procedures should also be implemented.**
 - Policies are kept on the Trusts staffnet website. During the staff departmental induction they are informed of where the policies are and which ones are specifically relevant to them. If there are any changes to policies or there are new policies implemented, staff are made aware of this via email and the staff newsletter. Managers will also mention any updates in team meetings, to inform staff who have not got access to email. However, no evidence of this was provided.
 - The Trust fully implemented Datix web in November 2016. Evidence has been provided showing that training and information has been given to all staff about this system and incident reporting in general. However, the Incident Management policy has yet to be updated with the new process for reporting incidents. The updating of this policy should be completed as soon as possible to ensure staff have guidance on what to do if an IG incident occurs.
- 4. The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and or damage.**
 - The Trust created an IG improvement plan after the undertaking was issued. This plan has identified key risks that the Trust needs to look into; one of which was risk management. It was reported that an element of this risk has been addressed by ensuring risk assessments are completed and reviewed for all of the Trusts information assets. However, the Trust has not provided evidence to confirm this new procedure. The Trust has also stated that they are now ISO27001 compliant, which should help with the implementation of measures to ensure the security of the personal data they process. However, there has been no ISO27001 certificate or other evidence provided showing this. There are also regular reviews of IG incidents at the Trusts IG Forum. If any trends occur from incidents, lessons learnt can be discussed in this arena.

2 May 2017 (follow-up to Undertaking issued 15 November 2016)

DPA – 7th Principle

On 19 April 2017 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by the London Borough of Ealing (LBE) in relation to the undertaking it signed on 10 October 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

LBE agreed to the undertaking following the Commissioner's investigation of an incident involving a social worker, who lost a court bundle containing sensitive personal data relating to 27 data subjects including 14 children, when she put them on top of her car and then drove off. The documents were not recovered (DPA – 7th Principle).

The ICO acknowledge that although the London Borough of Ealing has taken initial steps to address the requirements of the undertaking, significant work is still required before they are fully satisfied. In particular appropriate steps have not been taken to address the following requirements:

- 1. The council continue to work toward achieving their stated target for 100% completion of mandatory online data protection refresher training for all permanent, locum and temporary Social Care staff who handle personal data by 3 April 2017. That the same monitoring and recording processes for the completion of this training are applied to locum, temporary and permanent social care staff.**
 - LBE confirmed that 74% of social care staff (including permanent, temporary and locum) had completed the eLearning data protection module and 25% staff (without online access) had completed the PDF version between January 2016 and January 2017. Training was either part of induction for new starters or as a refresher course for existing staff. The remaining 1% were on long term absence. LBE reports that it is in the process of putting measures in place to ensure that any new starters since January 2017 complete the data protection module. There are currently no plans to ensure that the refresher training is completed annually.
 - It was difficult to obtain the training completion figures from LBE who confirmed they are derived manually by cross referencing names from the e-learning system and manual records of staff completing the PDF version of the course, with payroll lists of temporary and permanent staff. It is not clear how the ongoing control and monitoring of training will be achieved when managers do not have recurrent reports of training completion rates.
 - The council should implement management, monitoring and recording processes to verify that they have achieved and are maintaining their stated target for 100% completion of annual mandatory data protection refresher training for Social Care, locums, and temporary staff.

- 2. The recording and monitoring of initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data is performed as (1) above.**

- LBE have not established regular reporting and governance procedures to ensure data protection training compliance rates are maintained on an ongoing basis. Additionally it is unclear how training delivered via the PDF version of the module will be monitored. It is concerning that LBE advised that they may not monitor refresher training prior to the launch of updated training that will be required for GDPR.
- The council should implement monitoring and recording processes to assure that they continue to achieve their stated objective of 100% completion of annual data protection refresher training for all staff who are involved in the handling of personal data.

- 3. The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher Data Protection related training to meet the council's stated objective of an annual requirement.**

- The MetaCompliance review document states 'using the Policy Management software we are able to create and control business and IT policies, implement enforced compliance of key messages and monitor acceptance' and that 'Metacompliance is a robust mechanism for delivering and measuring refresher DP related training'. It was reported however that the tool is used to manage policy dissemination and it is not used for delivering and measuring the annual requirement to refresh the Data Protection e-learning training module.
- The council should therefore ensure that either MetaCompliance or another tool is a sufficiently robust mechanism for delivering and measuring refresher data protection related training to meet the council's stated objective of an annual refresher requirement.

If any further incidents involving the LBE are reported to the ICO, the undertaking and its fulfilment will be taken into consideration as part of its investigation process. Dependent upon the outcome, enforcement action could be considered by the ICO as a result.

18 May 2017 (follow up to Undertaking issued 4 November 2016)

DPA – 7th Principle

On 15 May 2017 the Information Commissioner's Office ('ICO') conducted a follow-up assessment of the actions taken by Royal Bank of Scotland ('RBS') in relation to the undertaking it signed on 4 November 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

RBS agreed to the undertaking following the Commissioner's investigation of an incident that took place in October 2014, whereby dozens of faxes containing personal data were sent to an incorrect fax number belonging to a third party organization, despite being informed that faxes were regularly being sent to the incorrect number over a period spanning over 14 months (DPA – 7th Principle).

The review demonstrated that RBS has taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, further work needs to be completed by RBS to fully address the agreed actions.

RBS confirmed that it has taken the following steps:

1. Procedures are put in place to ensure any reported breach of security relating to personal data is acted upon promptly and any containment and remedial measures are swiftly enforced;

- The process for breach reporting within the retail bank has been reviewed and amended to make it easier for staff reporting a data protection breach, including instances where communications have been sent to a recipient in error. An amended reporting form to log any data protection ('DP') breach was introduced in December 2016.
- RBS has provided evidence of the guidance it has issued on MyKnowledge; which is an online tool and is the front line/branch staff's first port of call for guidance on processes. This process has made it easy for staff to report a data protection breach. This guidance includes how to recognise a breach and contains a step by step guide including timescales, which stipulates that all breaches are required to be reported within 24 hours and where a breach meets the criteria for notification to the regulator, notification is to be submitted to the regulator within 72 hours.

2. Fax procedures are implemented consistently across all branches and regularly monitored to ensure consistent standards. Compliance with any associated fax policy and guidance should be monitored on an ongoing basis and appropriate steps taken to ensure any failings are rectified with minimal delay by no later than 24 February 2017;

- For those activities where there is currently no alternative to using faxes, RBS has provided evidence of the new fax procedure implemented in January 2017. The fax process includes the requirement to use pre-programmed numbers and any number added to the list must be double checked by a colleague.
- RBS has provided information on how the new process acts to enforce any remedial measures resulting from a fax data breach. As part of the new fax process, branch managers carry out a weekly check for any faxes sent in error to the wrong recipient and log them as a DP breach. The DP breach logs are continuously monitored by the business, via 'Privacy Champs' who sit throughout RBS' retail businesses. They check that appropriate corrective action is taken when DP breaches arise in their area and escalate any issues as required. The Privacy team further assesses all submissions on a monthly basis to spot trends and root causes, allowing for the identification of additional training and awareness needs. Monthly meetings are held with representatives across the retail bank. RBS states that attendees have been tasked with ensuring that Privacy matters are understood by their business areas with any areas of concern discussed and escalated to the Privacy team for guidance. However we have not been provided any evidence to support this.
- Evidence has been provided to show how RBS' Assurance teams have checked that the new fax process communication has been understood and is being implemented by their retail business, in the form of an Assurance thematic review which was conducted on 16 January 2017, three weeks after the implementation of the new fax process. This activity was completed by Control Quality Managers ('CQM') with support of the Business Embedding & Execution Managers across NatWest, Royal Bank of Scotland & Ulster Bank. The teams have visited 187 branches and spoken to 460 staff members.
- RBS has also provided a copy of the Faxed Themed Review Outcome dated February 2017. The results show that 88% of staff were aware of the new fax process, 96% of staff were able to locate the policy and 78% of staff were aware of the process to follow if they were informed by a customer or a third party of a data protection breach. A check of the pre-programmed numbers showed 67% were inputted correctly and 32% incorrectly. Of the numbers not pre-programmed, only 39% followed exceptions. According to RBS, the themed review failings in these areas have been addressed by either the CQM during their visit or through local actions plans, however no evidence has been provided to support this.

3. To ensure any alternative revised processes are fully tested for security and reliability and any related guidance is disseminated to all staff.

- At the time of the review, this action had not been completed. However, whilst no evidence has been provided to support the progress of this action, RBS appears to be considering more secure methods for transferring personal data.
- Work is presently under way to explore technical solutions which will allow switching from fax processes to electronic processes to allow for increased paperless processing within their branch network and telephony business. For example, the implementation of an email scanning solution is being pursued as the long-term alternative to using faxes.
- A phased roll-out is underway and is planned to complete in the first half of 2018. This project is a priority project for the retail bank. Before introduction of any new technical solution it will be fully tested in line with the Bank's standard processes and procedures and adequate controls put in place to protect customer data.
- RBS should ensure that as soon as practical, all staff handling personal data are provided with relevant guidance in relation to any newly implemented technical solution and trained in those new procedures, in order to safeguard customer's personal data.

4. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

- RBS carries out ongoing security awareness and education activities. Through these activities, RBS promotes and maintains a 'security aware' culture across the Bank that educates employees, contractors, third-party users, and business partners on how to protect bank information throughout its lifecycle. Employees are required to complete mandatory manual computer based training, guiding and reminding them of best practice.
- The need for security and confidentiality is addressed through Bank policy (such as the Bank's Security Policy and Privacy & Client Confidentiality Policy) including reminders to staff that data breaches must be promptly and fully internally reported once identified. A snapshot of the Security Policy dated 15 December 2016 has been provided, however this is not evidence of the above.
- In addition RBS' Security Policy requires the principles of least privilege and least access to be applied, to ensure that access is not authorised or available if there is no justified business requirement. Customers and Bank employees are identified and authorised before systems access is granted and access is regularly validated to ensure it remains appropriate.

However, RBS should take further action to fully address the agreed steps:

- RBS has provided evidence of the content of a new training session which is available online for staff to highlight the revised breach reporting process and the importance of logging DP breaches. Managers can access this material and deliver it to staff as and when a need for particular staff training is identified. However, no evidence has been provided to show how many staff have received this training. RBS should implement monitoring and recording processes to assure that all staff who handles personal data receives this training and that it is included in any mandatory refresher training.
- RBS has confirmed that staff are tested on their understanding of, and compliance with, the fax process on an ongoing basis. However, no evidence has been provided to confirm what percentage of staff have been tested, or whether any signed declarations are required from staff confirming their understanding of the new policy. RBS should therefore consider asking staff to sign a declaration to confirm their understanding of the new fax process and breach reporting procedure to ensure all staff are familiar with the new processes.
- RBS has confirmed that a further Assurance review into the new fax process will take place once adequate time has passed for recommended updates to be implemented, however no evidence has been provided as to when this review will take place and how often monitoring of compliance will be undertaken. Whilst we note that progress has been made in this area, we would strongly advise that the follow up review is conducted as soon as possible to ensure the identified failings are addressed promptly.

6 out of 11

undertakings were attributed to lack of staff training



3 July 2017

DPA – 1st, 3rd, 6th, & 7th Principles

In response to media reports publicised in May 2016, the Information Commissioner (the ‘Commissioner’) was alerted to an arrangement between the Trust and DeepMind Technologies Limited (‘DeepMind’), a UK company and data processor, under which DeepMind was engaged to develop and deploy a new clinical detection, diagnosis and prevention application for the Trust. The Commissioner launched an investigation which primarily focused on the data processing undertaken during the clinical testing phase of the application.

The investigation determined that on 30 September 2015, the Trust entered into an agreement with Google UK Limited (an affiliate of DeepMind) to develop and deploy a new clinical detection, diagnosis and prevention application and the associated technology platform for the Trust. In order to undertake clinical safety testing of this application and technology platform DeepMind, for this purpose and under the terms of the aforementioned agreement, processed approximately 1.6 million partial patient records containing sensitive identifiable personal information held by the Trust.

The identifiable information in question included information on persons who had presented for treatment at the Trust in the previous five years for pathology tests, together with data from the Trust’s existing radiology and electronic patient record system. The purpose of requiring DeepMind to process such information was to enable the clinical safety testing and deployment in live operation of a new application and associated technology platform that would provide the Trust with a mobile electronic patient record and an alert, diagnosis and detection system for acute kidney injury. The clinical safety testing of that platform was undertaken by the Trust, using the application and technology hosted and maintained by DeepMind.

The Trust explained to the Commissioner that clinical safety testing at the relevant time was required by standards issued under the Health and Social Care Act 2012 and needed to be undertaken before new technology was deployed. The Commissioner has concluded however that these points need further exploration before a final view can be reached on them and expects to find them considered more fully in the Privacy Impact Assessment that the Trust is required to complete.

The platform went on to be formalised into a mobile device application, known as ‘Streams’. From February 2017, the Streams application moved to live deployment and it is now in active use by the Trust’s clinicians. The Streams application is registered with the Medicines and Healthcare products Regulatory Agency as a Class I non-measuring device and is CE marked (a declaration of conformity with the EU’s Medical Devices Directive).

The agreement of 30 September 2015 set out the relationship between the Trust and Google UK Limited as one of a data controller to data processor, with the Trust retaining its data controller responsibilities throughout.

The Trust confirmed to the Commissioner that DeepMind was only provided access to patient records as a data processor. The Trust has also confirmed that DeepMind has never used that information for any purpose other than to conduct clinical safety tests and for the live operation of the application and associated technology platform set out above.

Data streaming between the Trust and DeepMind commenced on 18 November 2015. At that stage, the data was processed for clinical safety testing purposes only, and the Streams application was not in live deployment. This is an important point to note in the context of the conditions for processing that the Trust sought to rely upon at that stage.

All development and functional testing of the application and the related technology platform was undertaken by DeepMind using synthetic, non-personally identifiable, data. Pseudonymisation of the patient identifiable data was not undertaken for clinical safety testing. This is because the Trust was (and remains) of the view that it needed access to patient records in the application and technology platform in order to undertake clinical safety testing. The Trust is of the view that it is not possible to demonstrate clinical safety of a new technology of this type without access to information about real patients. The Trust was therefore of the view that the data was being held and made available for the purpose of direct patient care.

The Commissioner has concluded that there were a number of shortcomings in the way in which patient records were made available to DeepMind in support of the clinical safety testing of the Streams application by the Trust. These shortcomings amounted, in the Commissioner’s view, to non-compliance with the First, Third, Sixth and Seventh Data Protection Principles. These Principles are set out in Part I of Schedule 1 to the Act. The Commissioner considers that the data controller is also processing ‘sensitive’ personal data as defined by section 2(e) of the Act.

Principle One

The Commissioner’s investigation determined that DeepMind processed approximately 1.6 million partial patient records to enable the clinical safety testing of the Streams application by the Trust. It is the Commissioner’s view that patients were not adequately informed that their records would be processed for the purpose of clinical safety testing.

The Commissioner concluded that the data controller did not provide an appropriate level of transparency to patients about the use of their personal data during the clinical safety testing phase and that this processing was not something that the patients might reasonably expect. Specifically the Commissioner concluded that the fair processing information available to the patients was insufficient. Patients were not provided with sufficient notice that their records would be processed in support of the clinical safety testing of the Streams application. The Commissioner noted the recent improvements that have been made by the data controller to improve transparency and that a revised notice regarding live clinical use is now available.

The Commissioner was not satisfied that the Trust has, to date, properly evidenced a condition for processing that would otherwise remove the need for the Trust to obtain the informed consent of the patients involved for the processing of personal data for the clinical safety testing of the application prior to live deployment. As a result, during the Commissioner's investigation and to the Commissioner's satisfaction, the data controller has not been able to evidence a valid condition for processing personal data under Schedule 2 to the Act during the clinical safety testing phase of the application or to evidence a valid condition for processing sensitive personal data under Schedule 3 to the Act during the clinical safety testing phase of the application. The Commissioner therefore required the Trust to provide evidence that any future testing arrangements with DeepMind will comply with a processing condition in Schedule 2 and 3 to the Act.

The Commissioner worked closely with the Office of the National Data Guardian (the 'NDG') on the issue of whether the processing of the patient records during the clinical safety testing phase was in breach of the common law duty of confidentiality. The Trust maintains that the clinical safety testing of the application amounted to direct care so that it had the implied consent of its patients for confidentiality purposes, in accordance with the NDG's guidance. The Commissioner has considered the advice given by the NDG on this issue earlier this year and in light of the Commissioner's review and the NDG's view on the matter, the Commissioner considers it is likely that the processing of the records during the clinical safety testing phase was in breach of confidence and therefore not compliant with the First Data Protection Principle under the Act. The Commissioner has therefore required the Trust to provide evidence that any future development or testing arrangements with DeepMind are not in breach of its duty of confidence, as it relates to the First Data Protection Principle.

The Commissioner also notes that the Trust has adopted a revised notice and opt out approach, in line with the recent guidance of the NDG in order to enable compliance with patient confidentiality. Patients should also note that the Commissioner has not, in investigations to date, found grounds for concern regarding the data processing in the live use of the Streams application.

Principle Three

The Commissioner considered the Trust's representations as to why it was necessary for so many records (1.6 million) to be used to support the clinical safety testing of the application. The Commissioner was not persuaded that proper consideration was given to the necessity of processing so many patients' records. As such the Commissioner is of the view that the Trust has failed to demonstrate that the processing of such a large number of partial records was both necessary and proportionate to the purpose pursued by the data controller and that the processing was potentially excessive. The Commissioner did not receive evidence of whether lower volumes of records could have been used during the testing phase. Whilst the rationale for using the full range of records in the live clinical setting is now clearer, the Commissioner emphasises the importance of assessing the proportionality in future iterations of the application for testing or clinical purposes.

Principle Six

The Commissioner's investigation has determined that as patients were not provided with sufficient information about the processing and as a result those patients would have been unable to exercise their rights to prevent the processing of their personal data under section 10 of the Act. As set out above, the Trust has now taken further steps to ensure patients are aware of the use of their data for clinical safety testing and of their ability to opt out from such testing. This was not the case in 2015 and early 2016.

Principle Seven

Principle Seven requires that where a data processor carries out processing on behalf of a data controller, a contract evidenced in writing must be in place. Although there was a written information sharing agreement in place that set out the parties' roles and imposed security obligations on the processor at the time DeepMind was given access to the data, the Commissioner's investigation has determined that this agreement did not in the Commissioner's view go far enough to ensure that the processing was undertaken in compliance with the Act. It is the Commissioner's view that the information sharing agreement of 30 September 2015 did not contain enough detail to ensure that only the minimal possible data would be processed by DeepMind and that the processing would only be conducted for limited purposes. It is the Commissioner's view that the requirements DeepMind must meet and maintain in respect of the data were not clearly stated. The Commissioner is also concerned to note that the processing of such a large volume of records containing sensitive health data was not subject to a privacy impact assessment ahead of the project's commencement.

The Commissioner does however recognise that the Trust has since replaced and improved the documentation in place between the Trust and DeepMind and has increased patient visibility of the use of data for the Streams application.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the First, Third, Sixth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

1. The data controller will, within two months, complete a privacy impact assessment explaining how the data controller will demonstrate compliance with the Act in relation to the arrangement with DeepMind, if and to the extent such arrangement involves the processing of personal data relating to patients, during any future (a) application development and functional testing and (b) clinical safety testing that in either case is either planned or already in process. The privacy impact assessment should contain specific steps to review and (where necessary) ensure transparency and the provision of the fair processing information to affected individuals;

2. The data controller will, within one month of the date of the completion of the privacy impact assessment set out in (1) above, provide evidence that a condition for processing personal data under Schedule 2 to the Act applies in relation to its arrangement with DeepMind, if and to the extent such arrangement involves the processing of personal data relating to patients, to the use of such data for any further (a) application development and functional testing and (b) clinical safety testing which in either case uses patient data, and which in either case is either planned or currently in process;
3. The data controller will, within one month of the date of completion of the privacy impact assessment set out in (1) above, provide evidence that a condition for processing sensitive personal data under Schedule 3 to the Act applies in relation to its arrangement with DeepMind, if and to the extent such arrangement involves the processing of personal data relating to patients, to any future (a) application development and functional testing; and (b) clinical safety testing, which in either case is either planned or currently in process;
4. The data controller will, within one month of the completion of the privacy impact assessment set out in (1) above, provide the Commissioner with details of about how it will comply with its duty of confidence to patients as it relates to compliance with the First Data Protection Principle, in any future (a) application development and functional testing; and (b) clinical safety testing in relation to its arrangement with DeepMind if and to the extent such arrangements will use patient data and which in either case is either planned or in process;
5. The data controller will commission, within three months of the date of this undertaking, a third party audit of the current processing arrangements between the data controller and DeepMind, including an audit of how the data processing agreement between the data controller and DeepMind is operating, in practice in order to ensure compliance with Act, and disclose the findings to the Commissioner. The audit scope should assess both the current live clinical use of the Streams application and (a) any future application development and functional testing and (b) clinical safety testing that in either case is either planned or already in process. It should also include consideration as to whether the transparency, fair processing, proportionality and information sharing concerns outlined in this undertaking are now being met. The Commissioner will first approve the data controller's choice of auditor and agree the terms of reference. The Commissioner will, in the interests of transparency and in acknowledging the wider public interest in this case, retain the discretion to publish parts or all of the audit findings as appropriate.

9

of the undertakings
breached DPA principle 7



10 August 2017

DPA – 7th Principle

In February 2014, Cheshire West and Chester Council agreed to an ICO audit which was undertaken in October 2014, following which a limited assurance rating was achieved. A follow up was undertaken on behalf of the Commissioner in June 2015, to check progress with the agreed recommendations.

As a result of this audit and follow up, a number of concerns relating to staff training were identified. These concerns were compounded by a series of self-reported incidents which the Commissioner was advised of both during the follow up period to the audit and also thereafter. The majority of these incidents concerned disclosure in error cases and almost all staff involved who had not received data protection training. Some of these individuals were also temporary agency workers.

Despite agreed audit recommendations specifically related to training, which included the requirement to train all staff employed and monitor take up of such training, subsequent investigations have identified that these recommendations have not been implemented fully.

Further data breaches reported to the Commissioner subsequent to the audit follow up have involved disclosures which had the potential to cause serious distress for those affected, including: the disclosure of an incorrect mobile phone number to an ex-partner of a data subject; allegations of historic sexual abuse being sent to an incorrect address due to the address and postcode being obtained from a Google Map search. The data handling procedures introduced following previous breaches not being adhered to in some high risk areas as staff had not been made aware of it. Following investigations into those incidents, it was found that some staff members within these services had not received any data protection training at all.

Whilst the data controller has policies in place which highlight the data protection obligations of its employees, the level of overall organisational compliance with mandatory data protection training has fluctuated significantly over the last two years.

The latest organisational data protection training compliance figure for the year ended 2016/2017 was 61% overall, with much lower than expected attainment figures evidenced in some high risk areas such as Children and Family Services and Adult Social Care and Health.

Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follow:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. The data controller shall conduct a risk based training needs analysis for all roles within the organisation to ascertain the level of data protection awareness required for the role, and the frequency at which the individual should receive refresher training to ensure they are reminded of their obligations in order to prevent further security incidents. This analysis should also consider whether the training should be tailored for specific roles and should be completed within six months of the date of the undertaking.
2. The data controller shall deliver mandatory data protection training in relation to both the requirements of the Act and the data controller's policies and guidance to all employees whose role involves the handling of personal data, as identified in the training needs analysis and regardless of their contractual status. This process should be completed within six months.
3. The data controller shall ensure that all new members of staff responsible for the handling of personal data are given appropriate data protection training, commensurate with their role upon induction.
4. The data controller shall ensure that mandatory refresher data protection training is undertaken at the intervals identified and as set out in the training needs analysis; such training to be refreshed annually as a minimum.
5. The data controller shall ensure that mandatory data protection and refresher training is monitored and enforced.

10 August 2017 (follow-up to Undertaking issued 9 August 2016)

DPA – 1st Principle

On 21 June the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Kent Police in relation to the undertaking it signed on 8 August 2016. The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented.

Kent Police agreed to an undertaking following the Commissioner's investigation of an incident that involved downloading the entire contents of an individual's mobile phone, which contained a recording supporting the individual's abuse allegations, without informing the individual that this processing would take place. There was also no fair processing notice or other written authorisation form to explain to the data subject what she would be consenting to by providing her phone to the data controller (DPA – 1st Principle).

Findings of the ICO in relation to undertakings signed:

- 1. Develop written procedures and supporting documentation for the extraction of data from mobile devices which emphasise that explicit, informed consent should be sought from victims and witnesses of crime in the first instance by 31 October 2016.**
 - Written procedures have been documented for the extraction of data from mobile devices and they have been communicated to the teams and staff undertaking the work. The intranet was updated 16 October 2016 and further updates were made on 26 April 2017 with links to the process and fair processing form.
- 2. Create a fair processing notice for victims and witnesses of crime to read and sign, which clearly explains which personal data will be extracted from their mobile device and how this will be processed, by 31 October 2016.**
 - A fair processing form has been documented to include digital disclosures, version controlled and added to the documents repository. There are also links to the document via the intranet (InSite), briefing packs and local team communications. The use of the form, awareness and testing is frequently monitored in the form of on-site tests and audits.
- 3. Where technically possible, limit the extraction of data from the mobile devices from victims and witnesses of crime to relevant data sets and delete any irrelevant information once identified as such by the Disclosure Officer. The data controller shall ensure that these processes are contained within in the relevant written procedures by 31 October 2016.**
 - Kent police has made significant investment in resources to create dedicated digital hubs; one within each policing division. These environments will be secure with restricted and authorised access, staffed by fully trained operatives working to published policies and procedures which support compliance with all aspects of information and data management. The first phase of recruitment and training will be completed by the end of July 2017 and following a month of mentored operational activity, it is planned the organisation will be in a position to locally deploy staff to the three hub locations from 4 September 2017.
 - Three hubs have been established, two are in the process of being made operational and the third will be operational by November 2017.
 - A full review of staff able to complete digital downloads was conducted and resulted in a significant drop in numbers who are now able to undertake this activity. This is supported by regular audits and quality control checks.
- 4. Remain up to date with developments and guidance around the extraction of data from mobile devices and promptly take action to address any recommendations relating to compliance with the Act arising from this.**
 - As part of the monthly Force Security and Integrity Committee (FSIC) forum the forensics team will have visibility of updates to legislation and are included in the readiness for GDPR.
 - Work is ongoing to continually review and update policies and embed the guidance and continuously improve data protections standards with a structured audit program.
- 5. Implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**
 - The central forensic team have plans to safeguard data beyond the plans for forensic hubs and a collaborative approach facilitated by the Operational and Information Security (OIS) Head includes a broad audit program and regular forums to strengthen adherence to the Act.

27 September 2017

DPA – 7th Principle

The Information Commissioner (the ‘Commissioner’) was informed of several data protection incidents by Dyfed Powys Police over an 18 month period. The number of incidents reported is of concern especially as they are repeated in nature.

In August 2016, Dyfed Powys Police’s Mental Health Team passed sensitive personal data to an individual’s General Practitioner (GP). The information was sent by open fax message to the GP’s surgery, and whilst it arrived at its intended destination, appropriate consent was not obtained from the data subject. At the time of the incident the officer had not completed any data protection training.

The Commissioner’s enquiries into this incident revealed that as at 17 March 2017, 1,204 officers out of a total of 2,258 had not completed any data protection training and there was no current programme of refresher training in place.

In January 2017, an officer passed personal data relating to a Councillor and a neighbour by email to the clerk of a local council. There was no information sharing agreement in place between the data controller and the council; authorisation from a senior colleague was not sought prior to sending the email; and the officer had received no data protection training.

A third incident investigated by the Commissioner occurred prior to November 2015 but was not brought to the attention of the data controller and subsequently the Commissioner, until March 2017. The incident involved a photograph taken using a mobile telephone. The photograph showed an officer’s working environment, including a computer screen on which data was displayed. The picture was forwarded to a family member. By sending the photograph the officer breached the data controller’s Information Security Policy and the College of Policing Code of Ethics. The officer had received no data protection training.

The Commissioner’s investigation into these incidents has determined repeated failures with regard to the training of staff.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. A force-wide programme of data protection training adequate to equip officers with the necessary knowledge to comply both with the Act and with the data controller’s policies concerning the processing of personal data be implemented without further delay.
2. A force-wide programme of refresher training be introduced to ensure ongoing compliance with the Act.
3. A programme of recording and monitoring of training undertaken be implemented with prompt remedial action to address non-compliance being taken where necessary.
4. The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.
5. The data controller shall confirm its plans in writing to the Commissioner to demonstrate its commitment to these steps within one month of the date of agreement to this undertaking.

7

follow-ups to undertakings
issued in 2016





International Trends – Europe

1. Austria
2. Belgium
3. Cyprus
4. Czech Republic
5. Estonia
6. France
7. Germany
8. Gibraltar
9. Hungary
10. Ireland
11. Italy
12. Liechtenstein
13. Netherlands
14. Poland
15. Portugal
16. Romania
17. Switzerland

Total

17

Austria

Data Protection (Directive 95/46/EC)

Law – Austrian Data Protection Act ('DSG 2000'). This implements the EU Data Protection Directive.

Regulators – Data Protection Authority ('Datenschutzbehörde') and District Commission ('Bezirksverwaltungsbehörde' with civil and criminal courts).

Enforcement powers – via Data Protection Authority:

- Ombudsman proceedings (the Data Protection Authority can only make recommendations in these proceedings which are unenforceable)
- appeal proceedings (pursuant to the General Administrative Procedures if the data protection authority ascertains any illegality)

Penalties –

Law – The District Commission can impose penalties up to € 25,000.

Breach notification – According to DSG 2000 only the data subjects have to be notified of a data breach.

GDPR update

The Austrian legislator has made very limited use of the opening clauses e.g.

- Specified Data Protection Officer
- Data secrecy regulations
- Proceedings before the Data Protection Authority and appeal to the Federal Administrative Court
- Mandatory regulations including regarding data protection impact assessments and image processing
- Ability to impose fines on legal persons
- Data processing provisions for specific purposes (e.g. in the employment context)
- Data processing register continued until 31.12.2019 for archive purposes only

E-Privacy (Directive 2002/58/EC)

This is implemented by the Austrian Telecommunications Act ('TKG 2003'). The regulator is the Telecommunications Authority ('Fernmeldebüro'), whose enforcement powers are:

- Issuing, modification and revocation of authorisations for the establishment and operation of telecommunication or radio equipment; and
- Appeal proceedings (pursuant to the General Administrative Procedures)

The Telecommunications Authority can impose penalties up to €25,000.

NIS (Directive 2016/1148)

As at April 2018 the NIS Directive has not been implemented. The deadline for the implementation is 9 May 2018.

2017 notable issues

Breakdown of enforcement action

There is no publicly available data in Austria on data related enforcement activity or fines. The Austrian regulator has not issued any guidance or public statements about ongoing investigations or similar actions.

Insurance companies and banking institutions seem to be a particular focus of regulatory activity.

Litigation

Legal overview

Claims that may be brought by individuals – Generally the position in Austria is similar to the UK (i.e. claims can be brought under: data protection laws, breach of confidence, misuse of private information, defamation, harassment, employment laws).

Depending on the type of infringement, the data subject may bring:

- Civil law actions (e.g. employment law);
- Criminal law proceedings; and/or
- Administrative procedures or court proceedings.

Jurisprudence with regard to data protection breaches which constitute civil or criminal law proceedings is very limited in Austria. Usually, data breaches do not give rise to damages under the Austrian Civil Code however these will apply from 25 May 2018 onwards.

Key questions

Can damages be obtained for non-financial loss?

Not until 25 May 2018

Can claimants bring class actions? No

Are 'no-win-no-fee' arrangements available? No

Is third party litigation funding available? Yes

Has it been used for data protection claims?

No publicly available data in Austria.

What are the barriers (or perceived barriers) to litigation?

From an Austrian legal perspective, the data breach must (basically) lead to a violation of the right of the personality.

Other key developments

From 25 May 2018 onwards, data subjects may claim for so called 'non-material damages' (see art 82 GDPR). This is a novelty from an Austrian legal perspective and we assume that the numbers of this type of claims could rise.

The Austrian media are generally active in reporting on data protection related topics. So far there has been low media interest in data protection litigation. Privacy groups and lobbyists have expressed some interest in these issues and it appears that their activities are in the early stages.



Dr. Axel Thoss
+43 664 8863 9004
axel.thoss@pwc.com



Mag. Sabine Brunner
+43 664 8863 9015
sabine.brunner@pwc.com

Belgium

Data Protection (Directive 95/46/EC)

National Law – the Belgian Privacy Act is the main law for implementing the EU Data Protection Directive.

Regulator – Belgian Privacy Commission.

Enforcement powers – The Belgian Privacy Commission has powers to:

- investigate (on the basis of complaints or on its own initiative); and
- demand civil and/or criminal sanctions before court.

Penalties –

Law – The criminal sanctions a court can impose include:

- fines up to EUR 600k;
- confiscation of the data carriers involved in a privacy violation;
- obligatory erasure of data; and
- prohibition on managing any data processing for a 2 year period.

Imposed – To date Belgian courts have not yet imposed any criminal sanctions for privacy law breaches.

Breach notification – Only mandatory for enterprises that offer public electronic communication services (see below regarding the E-Privacy Directive).

GDPR update

At present, government bills are being introduced to reform Belgian law and align it to the provisions of the GDPR.

Currently, it looks like criminal sanctions will continue to exist under Belgian privacy law. In addition to the GDPR, Belgian law enacts specific provisions with respect to the monitoring of employees ('cyber surveillance') and the transfer of personal data between government agencies (as necessitated under various authorisation applications).

Post-GDPR the Belgian regulator will be the Data Protection Authority ('Gegevensbeschermingsautoriteit'/'L'Autorité de Protection des Données').

E-Privacy (Directive 2002/58/EC)

This relates to electronic communications and has been implemented in Belgium through various acts (e.g. the Telecom Act). It covers the processing of personal data and is regulated by the Belgian Privacy Commission with the same powers and potential penalties as listed above.

NIS (Directive 2016/1148)

As at April 2018 there is no information available on if or how this will be implemented, or who the regulator(s) may be.

2017 notable issues

Break-down of enforcement action

Type	No.
Inspections	332

Information has not been made public about the number of other types of data related enforcement activity.

In 2017, the Belgian Privacy Commission had not taken significant enforcement actions and had not demanded civil and/or criminal sanctions before court.

The Belgian Privacy Commission has concentrated on issuing draft guidance in preparation of implementation of the GDPR and issuing recommendations with respect to the processing of personal data such as in the fight against terror (e.g. transfer of biometric data of perpetrators of criminal behaviour to the United States) and the fight against energy fraud (e.g. use of data mining to detect fraud).

Notable enforcement action/investigations concluded

Facebook

Date of enforcement: 2015

Industry – Media

Incident – The Belgian Privacy Commission initiated proceedings against Facebook for an alleged infringement of the information obligation of Facebook (as a controller) towards users and non-users (data subjects).

The Belgian Privacy Commission found that Facebook did not adequately inform certain data subjects (non-Facebook users) on the processing of personal data performed by Facebook (e.g. which data was collected and the purposes for which their data is processed) and that it could not rely on a lawful ground for the processing of certain data such as lack of consent.

Observations – In February 2018, the court of first instance in Brussels ruled that this processing conducted by Facebook constituted an infringement of the privacy rights of data subjects, in particular as insufficient information was provided to the data subjects, along with a lack of lawful grounds for the processing concerned. The court ruled that Facebook should cease the unlawful processing and destroy all unlawfully acquired data. If Facebook fails to comply with this court order it will be required to pay a penalty payment of EUR 250k per day, up to a maximum of EUR 100 million.

Other key developments

Enforcement trends – Cross-border cooperation between supervisory authorities and cross-border coordination of enforcement actions (e.g. Yahoo, Whatsapp).

Sector focus – Government institutions, Marketing, Telecoms, New technologies (e.g. use of big data, IoT, mobile apps).

Litigation

Legal overview

Claims that may be brought by individuals – Claims can be brought for breach of the following areas of law: data protection, employment, electronic communication, health care, consumer, civil law (breach of confidence) criminal law (professional secrecy, defamation, misuse of information, breach of confidence), and cybersecurity (critical infrastructure).

Litigation with respect to data protection breaches is still very underdeveloped in Belgium and some of the available claims listed above have not yet been used.

Key questions

Can damages be obtained for non-financial loss?

Yes, this is possible but subject to case by case analysis.

Can claimants bring class actions?

No, in principle class actions are not permitted under Belgian law. There are some limited exceptions, but they do not cover claims arising from data protection law.

Notable case

Claimant(s): Belgian Special Tax Inspectorate

Defendant(s): International payment service provider

Industry – Finance, insurance and credit

Causes of action – The Specific Tax Inspectorate (“STI”) requested billions of transactional data regarding electronic payments conducted in Belgium from various payment service providers in the context of the fight against tax fraud.

Mitigating/aggravating factors – The STI requested a large amount of personal data which was unlikely to be relevant for the purposes of the investigation and was likely to concern special categories of personal data.

Significant points of law – Proportionality of processing and less intrusive alternatives, reasonable expectations of the data subject.

Judgment – The court ruled that the request for information was not proportionate and therefore violated the right to the protection of privacy and the right to the protection of personal data as the STI requested a lot of information that was unlikely to be relevant. Furthermore, the STI failed to demonstrate that no other less intrusive measure could be relied upon to lower the impact on the privacy of the data subjects.

Other key developments

Media interest – High levels of interest, for example several recommendations and interventions by the Belgian Privacy Commission made front page news in 2017.

Privacy groups/lobbyists – are interested in data privacy matters, for example consumer organisations.

Guidance – No data regulatory guidance has been issued during 2017.



Carolyn Vande Vorst

+32 496 275129

carolyn.vande.vorst@lawsquare.be



Leen Van Goethem

+32 485 233682

leen.van.goethem@lawsquare.be

Cyprus

Data Protection (Directive 95/46/EC)

National Law – The Data Protection Directive has been transposed into Cyprus law via the Processing of Personal Data (Protection of Individuals) Law 138 (i) 2001 (the 'Data Protection Law').

Regulator – Office of the Commissioner for Personal Data Protection.

Enforcement powers:

- To issue warnings;
- To grant relevant licences under the Data Protection Law;
- To report any contraventions of the provisions of the Data Protection Law to competent authorities;
- To impose administrative sanctions (including but not limited to monetary fines, revocation of license (temporary or permanent), destruction of database and cessation of processing activity; and
- To conduct an administrative inquiry on any filing system.

Penalties –

Law – The maximum financial penalty is €30,000.

Imposed – The largest penalty to date was for €10,000.

Breach notification – Not mandatory. There are no provisions in the Data Protection Law regulating mandatory breach notification.

GDPR update

A new law will be enacted which shall repeal the Data Protection Law and shall facilitate the better application of certain provisions of the GDPR.

The Office of the Commissioner for Personal Data Protection will continue to be the regulator for this new law.

E-Privacy (Directive 2002/58/EC)

The Directive was transposed into Cyprus law via the Regulation of Electronic Communications and Postal Services Law, Law 112(I)/2004 (the 'E-privacy Law').

The regulator for the Directive is the Office of the Commissioner for the Regulation of Electronic Communication and Postal Services (the 'Commissioner'). The Commissioner can:

- Regulate by order, decision or any interim measure the access and interconnection all consumer related issues and all other matters which fall within the Commissioner's competence; and
- Imposes fines and other penalties up to €342,000.

The largest penalty to date was €100,000.

Breach notification is mandatory.

NIS (Directive 2016/1148)

The Security of Networks and Information Systems Law of 2018 will implement the NIS Directive in Cyprus.

2017 notable issues

Breakdown of enforcement action

Notable enforcement action/investigations concluded

Date of enforcement: 25 March 2018

Industry – Local government.

Incident – Making of telephone calls and instant messaging of a political and promotional nature to voters during the pre-election period of the Cyprus presidential campaign.

Enforcement action – Several monetary fines to a number of presidential candidates amounting to €64,000.

Observations – The fines may not be considered significant enough to prevent future similar breaches.

Cyprus Telecommunications Authority (CYTA)

Incident – Unauthorised access of personal data by employees of the company and the subsequent unauthorised disclosure of the same to a third party.

Observations – The monetary fine was relatively low.

Litigation

Legal overview

Claims that may be brought by individuals

Please note that under Cyprus law, any person who suffers harm as a consequence of a breach of applicable data protection law can initiate a civil action for damages.

Key questions

Can damages be obtained for non-financial loss? Yes

Can claimants bring class actions?

Class actions are not permitted under Cyprus Law.

Are 'no-win-no-fee' arrangements available? No

Is third party litigation funding available?

As far as we are aware third party litigation funding, has not yet been tested or considered by Cypriot Courts.

What are the barriers (or perceived barriers) to litigation?

Delay and cost may discourage litigation.



Spyros Evangelou
+35 722 559900
spyros.evangelou@cy.pwclegal.com



Glafcos Kyprianou
+35 722 559712
glafcos.kyprianou@cy.pwclegal.com

Czech Republic

Data Protection (Directive 95/46/EC)

National law – the Czech Republic has implemented the EU Data Protection Directive.

Regulators – The Office for Personal Data Protection (Úřad pro ochranu osobních údajů).

Enforcement powers – Enforcement through remedial measures and penalties.

Penalties –

Law – CZK 10,000,000.

Imposed – CZK 4,250,000.

Breach notification – Yes, in case of providers of electronic communications services; according to the Cyber Security Act.

GDPR update

The new act on personal data protection has not been adopted yet. It is currently in the legislative process. It will be regulated by The Office for Personal Data Protection.

E-Privacy (Directive 2002/58/EC)

The Czech Republic has implemented the E-Privacy Directive. The regulator for the Directive is the Czech Telecommunication Office (Český telekomunikační úřad), which has the power to impose penalties. The maximum financial penalty under the Act on Electronic Communications is CZK 50,000,000. Notification of serious breaches is mandatory.

NIS (Directive 2016/1148)

The Czech Republic is implementing the NIS Directive mostly through amendments to the Cyber Security Act. The regulator will be the National Cyber and Information Security Agency (Národní kybernetický úřad).

Sector-specific regulation

There are some additional acts which regulate cyber security or liability, for example the Act on Information Systems of Public Administration. The regulator for these purposes is the Ministry of Interior, which has the power to impose financial penalties up to CZK 1,000,000. There is no mandatory breach notification in this specific regulation.

2017 notable issues

Breakdown of enforcement action

Notable enforcement action/investigations concluded.

Stellart S.R.O.

Date of enforcement: 21 September, 2016

Industry – Health.

Incident – Loss of client health data.

Mitigating/aggravating factors –

Mitigating factors: Removing of the malfunction.

Aggravating factors: Concerned sensitive personal data.

Enforcement action – Penalty was imposed.

Other key developments

Sector focus – Anti-vendor lock-in – The Office for the Protection of Competition (Úřad pro ochranu hospodářské soutěže) issued information regarding technical barriers in cloud services data portability. This was amended as part of the Cyber Security Act and the Act on Information Systems of Public Administration (2017).

Litigation

Legal overview

Claims that may be brought by individuals – Claims can be brought by individuals under the data protection laws, for breach of confidence, misuse of private information, defamation, harassment, employment laws and under the criminal code.

In the case of a violation of the rights of the data subject in connection with personal data, the data subject may contact The Office for Personal Data Protection. In the case of an offence under the Criminal Code, it is possible to file a criminal complaint. In any other case, an action may only be brought in a civil court.

Key questions

Can damages be obtained for non-financial loss?	Yes
---	-----

Can claimants bring class actions?	
------------------------------------	--

Not in the true sense (according to the US doctrine).	
---	--

Are 'no-win-no-fee' arrangements available?	
---	--

Yes, such business models do exist but are not specifically regulated by any law.	
---	--

Is third party litigation funding available?	
--	--

Yes, such a model exists, but it is not specifically regulated in any law.	
--	--

What are the barriers (or perceived barriers) to litigation?	
--	--

Court fees and the long duration of trials.	
---	--

Other key developments

Media interest – GDPR and the proposed consequences and fines and the readiness of controllers who do not yet comply with the current national legislation. Current national legislation is mostly ignored as the fines under it were not imposed.

Guidance – The Office for Personal Data Protection (has issued some basic guidance, including the 'Basic Manual' and a 'Q&A'.



Milan Fric

+420 703 186 917

milan.f@pwc.com

Estonia

Data Protection (Directive 95/46/EC)

National Law – the Estonian Personal Data Protection ('PDPA') has implemented the European Data Protection Directive.

Regulator – Estonian Data Protection Inspectorate ('DPI').

Enforcement powers – The main functions of the DPI are:

- Monitor compliance with the requirements provided by the PDPA;
- Apply administrative coercion on the bases, to the extent, and pursuant to the procedures provided by law;
- Initiate misdemeanour proceedings where necessary and impose punishments;
- Co-operate with international data protection supervision organisations, foreign data protection supervision authorities and other competent foreign authorities and persons;
- Give instructions of an advisory nature for application of the PDPA; and
- Perform other duties provided by law.

In performing its functions, the DPI has many rights including:

- Issuing principles to processors of personal data and adopt decisions for the purposes of ensuring compliance with the PDPA;
- Upon failure to comply with a principle, the DPI may impose a penalty payment pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act;
- Imposing fines;
- Suspending the processing of personal data;
- Demanding the rectification of inaccurate personal data;
- Prohibiting the processing of personal data;
- Demanding the closure or termination of the processing of personal data, including destruction or forwarding to an archive; and
- Where necessary, immediately applying, in order to prevent the damage to the rights and freedoms of persons and organisations and implementing physical or information technology security measures for the protection of personal data pursuant to the Substitutive Enforcement and Penalty Payment Act, unless the personal data is processed by a state agency.

In order to exercise state supervision provided for in the PDPA, the DPI may apply the specific state supervision measures provided for in sections 30, 31, 32, 49, 50 and 51 of the Law Enforcement Act on the basis of and pursuant to the procedure provided for in the Law Enforcement Act.

The DPI may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages.

Upon the exercise of administrative supervision, competent officials of the DPI have the right to enter, without hindrance, the premises or territory of a processor of personal data, demand relevant documents and other necessary information from persons, make copies of documents and access the equipment of a processor of personal data as well as the recorded data and the software used for data processing.

Penalties –

Law – Under the PDPA, the maximum fine for violation of personal data processing requirements for legal persons is EUR 32,000. The maximum rate for penalty payment is EUR 9600.

Imposed – The maximum fine issued for misdemeanour has been EUR 600 (in 2014).

Breach notification – No, not a general one under the PDPA.

GDPR update

Currently Estonia have the draft Personal Data Protection Act that has been heavily criticised and has not been adopted yet. Recently also the draft Personal Data Protection Implementation Act was published.

In addition, changes are being made to the Penal Code and to other laws concerning the legal consequences of misdemeanour proceedings. These modifications are important to enable DPI to initiate fines according to the maximum rates that have been established in the GDPR. However, it has not been adopted yet.

Post GDPR, the regulator will continue to be the DPI.

E-Privacy (Directive 2002/58/EC)

- The E-Privacy has been implemented through the Electronic Communications Act ('ECA').
- The regulator is different; and
- The enforcement powers/mechanisms are controlled through state and administrative supervision which is exercised by different authorities (see Chapter 13 of the ECA).
- State and administrative supervision of compliance with the personal data processing requirements are provided for in the ECA. They also supervise the use of electronic contact details provided for in the ECA and where appropriate administrative coercion shall be applied by the DPI.
- Extra-judicial proceedings concerning the misdemeanours under the ECA are conducted by different authorities, depending on the misdemeanour (see section 188 and Chapter 14 of the ECA).
- Extra-judicial proceedings concerning the violation of the confidentiality of information concerning the user, which has become known in the process of provision of communications services, or failure to give notice thereof is conducted by the DPI.
- The maximum fine for the violation of is EUR 2000 (for legal persons). For others, see Chapter 14 of the ECA.
- Regarding mandatory breach requirement the ECA states that if a specific hazard exists to a communications service or the security of the communications network, the network must immediately inform the subscriber of such a hazard in a reasonable manner. Unless the hazard can be eliminated by through certain measures it should inform the subscriber of possible remedies and of any costs related thereto.
- Also, in the event of a personal data breach, a communications undertaking is required to notify the DPI at the earliest opportunity.

NIS (Directive 2016/1148)

- Estonia is most likely to implement the NIS Directive through the Cyber Safety Act which is set to be adopted. Currently the draft of the Cyber Safety Act has been submitted to the Parliament of Estonia.
- The regulator will be the Estonian Information System Authority.

Sector-specific regulation

Finance, insurance and credit

- The Financial Supervision Authority ('FSA') regulates and has issued guidelines on the IT security requirements for financial institutions, including incident notification (effective as of 1 May 2018).
- The FSA's enforcement powers include the right to receive information from subjects of financial supervision for exercising supervision. In the guidelines, the FSA asks companies to provide the information listed below regarding any incidents. Under the Credit Institutions Act ('CIA'), the FSA has a vast number of enforcement powers (see Chapter 9 of the CIA), including the power issue rules, penalty payments and fines.
- In the event of a failure to comply with or inappropriate compliance with an administrative act, the upper limit for a penalty payment is, in the case of a natural person, EUR 5,000 for the first occasion and up to EUR 50,000 for subsequent occasions. The FSA can enforce more than one fine, but together these cannot exceed more than EUR 5,000,000 or in the case of a legal person, up to EUR 32,000 for the first occasion and EUR 100,000 for each subsequent occasion. Also, in order to enforce the performance of one or more obligations, the fine cannot exceed more than 10% of the net annual turnover of the whole legal person, including gross income which, in compliance with Regulation (EU) No.575/2013 of the European Parliament and of the Council, consists of commissions and fees and interest and other similar income.
- Under the CIA, failure to make public or submit to the FSA a mandatory report, document, explanation or other data provided for in the CIA or Regulation (EU) No 575/2013 of the European Parliament and of the Council in a timely manner, or submission of an inaccurate or misleading information or publication thereof, if committed by a legal person, is punishable by a fine of up to EUR 32,000.
- According to the FSA guidelines there is a mandatory breach notification and financial institution should inform FSA as soon as possible of major incidents (i.e. incidents that regard personal data) by forwarding as much information about the incident as possible at the time of informing. The financial institution should also present the FSA with description of the occurrence at least three days after by using general contact information and noting the following information:
 - Type of incident (availability, integrity, confidentiality); Time of occurrence of the incident;
 - The scope and effect of the incident;
 - Description of the incident;
 - Cause of the incident;
 - Solution of the incident; and
 - Measures that are planned to be enacted for the prevention of similar incidents in the future.

Health

- The Emergency Act regulates the organisation of continuity of vital services and states rules for ensuring electronic security of provision for vital services.
- The regulator is the Estonian Information System Authority
- Its enforcement powers include issuing rules, penalty payments and fines.
- Upon failure to comply with a rule the upper limit for a penalty payment for each imposition pursuant to the procedure in the Substitutive Enforcement and Penalty Payment Act is EUR 2000.
- According to the Emergency Act, violation of the requirements of electronic security for the provision of a vital service is punishable by a fine up to EUR 800 (200 fine units). For legal persons the maximum fine is EUR 20,000.
- As the Emergency Act is very new there have been no penalties issued to date.
- There is a mandatory breach notification under a Government Regulation adopted under the Emergency Act. A provider of vital services must notify the Estonian Information System Authority without delay.

2017 notable issues

Break-down of enforcement action

Type	No.
Monitoring procedures initiated by DPI	149
Inspections	45
Recommendations	125
Precepts (incl. warning of applying coercive measures)	64
Misdemeanour procedures	9
Penalties imposed ¹	4

¹ Incl. those imposed in misdemeanour procedures, but also penalties imposed as coercive measures

Public Sector	No./EUR
Fines	2
Penalty payments	0
Recommendations	125
Highest fine	EUR 80
Total value	EUR 140

Private Sector	No./EUR
Fines	0
Penalty payments	2
Highest penalty payment	EUR 1,500
Total value	EUR 3,000

Notable enforcement action/investigations concluded

Estonian Human Rights Centre

Date of enforcement: December 2009

Industry – Charitable and Voluntary

Incident – Estonian Human Rights Centre ('EHRC') operated an application UNI-FORM that focuses on hate crimes against LGBTI people (lesbian, gay, bisexual, and transgender, intersexual). The platform is meant for all the victims, witnesses and other people, who wish to report an incident, which has been caused by prejudice (i.e. sexual orientation, sexual identity or sexual expression). Reports based on that information may be anonymous or even include personal details, which makes it possible to actually start proceedings based on the given information. If contact details have been provided, a specialist of EHRC contacts the person, who has notified about an incident through the app, and provides counselling.

Foundation for the Protection of Family and Tradition ('FPFT') filed a complaint to the Data Protection Inspectorate, asking to check whether the EHRC mobile app is in compliance with the Personal Data Protection Act. FPFT was concerned that EHRC does not have legal grounds for processing such personal data that the reports may include. They were especially worried about the fact that EHRC was processing sensitive personal data.

DPI initiated monitoring procedure, which is currently pending.

Other key developments

Enforcement trends – The DPI Director-General recently explained the main focus of the DPI is, to prevent violations by raising awareness of the data processing rules and advising people in different sectors, instead of imposing huge penalties. He explained that penalties have always been the last resort, which are justified in case of a serious, malicious and/or continuing violation. In case of a violation, the DPI first issues a warning or a condition. According to the Director-General, usually the condition is complied with and there is no need to impose fines. Although the GDPR changes the rates of possible penalties, the DPI is not planning to change its policies by prioritising the imposition of penalties.

Sector focus – The DPI conducts monitoring regarding different processing activities in different sectors and does not focus on any particular sectors or industries.

The DPI also conducts audits of the history which shows somewhat of a focus on the health care sector.

Litigation

Legal overview

Claims that may be brought by individuals – In Estonia claims can usually be brought under:

- Data protection laws;
- Defamation;
- Discrimination;
- Penal Code; and
- Employment laws.

Although possible to claim compensation for pecuniary damages (in addition to non-pecuniary damages) in defamation cases, courts usually do not award such compensations.

Concerning unauthorised disclosure of personal data (related to work), Estonian courts have said, that pecuniary damages (incl. loss of profit) may be awarded, if the claimant provides proof that the disclosure of his/her data has been unlawful (according to the LOA), claimant has suffered damages and there is a sufficient link between the disclosure and the damages.

In a case, where a person was not hired because his/her previous employer sent some negative personal information to the new employer, the court decided that the claimant had provided enough evidence to show that he/she had suffered loss of profit. The claimant had provided proof of an e-mail where he/she was offered EUR 10,500 per month and was also informed that he/she was a successful candidate. As the claimant was first offered a 1 year contract, the court agreed that 12 months multiplied by monthly salary minus taxes on labour, his/her current salary and other costs which would have been borne if he/she had moved to another country, as a substitute for loss of profit and patrimonial damages must be awarded.

(Tallinn Circuit Court 17.01.2017 decision 2-15-9284)

Data Protection Claims – According to the Personal Data Protection Act, if the rights of a data subject have been violated upon processing of personal data, the data subject has the right to demand damages. These claims are not very common in Estonia.

Defamation Claims – According to the Law of Obligations Act ('LOA') if personality rights have been violated (including defamation of a person), the aggrieved person has the right to demand damages and also demand from the person who disclosed incorrect information that they refute such information or to publish a correction (this only applies when the information is factual, i.e. is not a judgement based on value). An aggrieved person cannot in any case demand an apology for publishing incorrect information or defamatory value judgements. These claims are pursued frequently in Estonia.

Discrimination Claims – According to the Equal Treatment Act, if the rights of a person are violated due to discrimination, he/she may demand from the person who violates the rights that discrimination be discontinued and compensation be paid for the damage caused to him/her by the violation. These claims are not very common in Estonia.

Penal Code Claims – Some actions classify as criminal offences or misdemeanours according to the Penal Code and are punishable. Such offences include unauthorised surveillance, illegal disclosure of personal data (in the course of professional activities), illegal disclosure of sensitive personal data and illegal use of another person's identity. It is not very common to start such proceedings in Estonia.

Employment Claims – An employee has the right to access the information gathered about him or her by the employer and demand the employer that incorrect information be removed or corrected. This however is not a significant basis for a claim, as it just repeats the same rights every individual has under the data protection laws.

Key questions

What is the largest award of damages to date?

- To our knowledge, EUR 10,000. This was a defamation case, where an Estonian politician was called a corruptor in a newspaper and was associated with some fraud scheme. The court argued, that because of the huge revenue of the newspaper, a small award would not prevent further violations of this kind. Before this case, the largest award for nonpecuniary damage had been EUR 5000. We do not have any data as regards to material damages.
- In defamation cases there are rarely pecuniary claims, i.e. loss of profit or direct monetary damages, because these are cumbersome to prove if not impossible. Therefore aggrieved persons tend to limit their claims to non-pecuniary damages. However, it is also possible to demand compensation for legal fees that a person has paid before initiating any court proceedings.

Can damages be obtained for non-financial loss? Yes

Can claimants bring class actions?

- Estonia does not have the concept of class actions as understood in common law countries. In Estonia, it is not allowed (especially in civil cases) for a person to bring an action to the court in the name of other persons (especially if they are not aware of their own claim), who have been damaged in the same way without any transfer of claims. The basic principle is that a person must themselves file a claim to protect his or her rights.
- In civil matters the court conducts proceedings in a civil matter if a person files a claim with the court pursuant to the procedure provided by law for the protection of the person's alleged right or interest protected by law. In the cases prescribed by law, the court also conducts proceedings in a civil matter if a person files a claim with the court for the protection of a presumed right or interest protected by law of another person or the public. These are usually the cases provided in family law (guardianship matters and transactions with the assets of a person under guardianship). An exception is the right of the Consumer Protection Board ('CPD') to demand through court that the application of standard terms, which cause unfair harm to the collective interests of consumers and unfair commercial practices, be prohibited.
- To our knowledge, there are no such cases regarding personal data protection prescribed in law (except with the CPD which can represent consumers in the abovementioned occasions.)
- The submission of a joint action by several plaintiffs is allowed.
- Individuals may have recourse to an administrative court only for the protection of their rights. For other purposes, including protection of rights of another person or protection of a public interest, a person may only have recourse to the court in the cases provided in the law (usually regarding environmental disputes and planning procedures).
- To our knowledge, there are no such cases regarding personal data protection prescribed in law.

Are 'no-win-no-fee' arrangements available? Yes

Is third party litigation funding available? Yes

What are the barriers (or perceived barriers) to litigation?

- High costs and low amount of nonpecuniary damages (due to a very conservative approach in the court practice);
- Lack of knowledge; and
- Providing proof of the damages.

Notable cases

Claimant(s): Eerik-Niiles Kross

Defendant(s): AS Äripäev

Industry – Other.

Causes of action – Defamation. Claimant was called a corruptor in a newspaper.

Mitigating/aggravating factors – The newspaper argued that the claimant had been involved in some fraud schemes. The claimant argued that the information published in the newspaper was unjustified and damaged his reputation.

Significant points of law – The LOA sections 1046 (1) and 1047 (1) establish that it is possible to damage somebody's reputation by passing undue value judgement or by disclosing incorrect information (also incomplete or misleading information).

LOA section 134 (2) states that in the case of defamation of a person, the aggrieved person shall be paid a reasonable amount of money as compensation for non-patrimonial damage.

Judgment – Court was satisfied with the action and ordered the defendant to pay EUR 10 000 EUR to the claimant.

Legal costs – No information given in the judgment.

Observations – Historically Estonian courts have been very keen on the previous case law that concerns the amounts of compensation for non-patrimonial damage. However in this case the court was bold enough to change the established case law by awarding a significantly larger amount of damages than in previous cases (previously the highest amount had been EUR 5,000).

It should be taken into account that this court decision was made by the lower courts in Estonia, i.e. the Supreme Court did not accept the appeal. This decision was also very strongly criticised by some of the media law experts. One point in question was that the courts did not regard the fact the aggrieved party was a high-class politician who, at the time of the defamation, was running for the mayor of Tallinn and represented anti-corruption ideals, but at the same time is a businessman with shady connections, which was proven by the media organisation.

Other key developments

Media interest – Litigation concerning unlawful publication of someone's data in media and defamation cases, are often mentioned in newspapers. Usually these cases concern politicians and other public figures.

Media interest – Currently the main headlines in media concern the uncertainties caused by the new regulations provided in the GDPR.

Guidance – The DPI has issued general guidelines on breach notification. The DPI has notified that it will create a web service on its web page to facilitate the submitting of breach notifications.



Mari-Liis Orav

Attorney-at-law

+372 515 4388

mari-liis.orav@pwc.com

France

Data Protection (Directive 95/46/EC)

National Law – Act n° 2004-801 of 6 August 2004. This transposed the EU Data Protection Directive into national law.

Regulators – The National Commission for Data Protection and Liberties ('CNIL') created in 1978 by the French Law n° 78-17 of 6 January 1978 ('Loi Informatique et Liberté') (Data Protection Act).

Enforcement powers – The CNIL verifies the compliance of laws by performing investigations and inspections such as on-site inspections, oral or online hearings, but also online investigations.

During on-site inspections, the CNIL may request any relevant documents, access any business premises, request any documents, hear any employees, and also have access to computer programs and data.

The CNIL may decide potential sanctions and may issue formal notices. The CNIL may also inflict various administrative sanctions, especially financial penalty. The sanction can be made public. The CNIL may also impose an injunction to cease or to stop the processing and/or a withdrawal of the authorization granted by the CNIL.

In the event of serious and immediate infringement of rights and freedoms, the chairman of the CNIL may request the competent Court to order any necessary measure.

The CNIL may inform the Public Prosecutor of any infringement of data protection laws. The Public Prosecutor may also be seized despite transmission of documents regarding infringements to the litigation department of the CNIL.

Penalties –

Law – French Law n° 2016-1321 of 7 October 2016 ('Loi pour une République numérique') increased the level of financial penalties from 150,000 euros to 3 million euros.

Breaches of data protection could constitute criminal offences and may carry up to 5 years' imprisonment and fines up to 300,000 euros, depending on the infringement. Legal entities being held liable for breaches of data protection face a criminal penalty up to 1.5 million euros.

Imposed – The largest penalty to date is 150,000 euros. (c.f. Facebook case infra).

Breach notification – Yes, however mandatory breach notification is limited to providers of electronic communication services, as defined under Article L. 33-1 of the Electronic Posts and Communications Code (examples: Internet service providers, fixed or mobile telephone operators).

GDPR update

The French Data Protection Act of 1978 will not be abolished, only amended by an upcoming law.

The new French draft law dated 13 December 2017 will supplement enforcement under GDPR. This draft law is still under discussion within the French Parliament.

E-Privacy (Directive 2002/58/EC)

The E-Privacy Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector was transposed in French law.

NIS (Directive 2016/1148)

The NIS Directive 2016/1148 of 6 July 2016 on security of network and information systems was transposed in French Law by Act n° 2018-133 of 26 February 2018.

The CNIL and the National Information Systems Security Agency (ANSSI) will be the French regulators.

The ANSSI is the national authority in charge of accompanying and securing the development of digital technology.

2017 notable issues

Breakdown of enforcement action

Industry	Number of fines	Total value (€000's)
Health	1	10
Online technology and telecoms	2	175
Other: Waterproofing work	1	1
Transport and leisure	2	55
Total	6	241

Notable enforcement action/investigations concluded

Facebook inc and Facebook Ireland

Date of enforcement: 27 April 2017

Industry – Online technology and telecoms

Incident – In 2015, following the announcement by Facebook of the change in its policy for data use, the CNIL conducted various investigations into the social network's compliance with the Data Protection Act and identified several breaches of law.

These breaches concerned the massive processing of personal data of users for the purposes of advertising and the tracking of users without prior information, with or without a Facebook account, on third party sites via cookies.

Mitigating/aggravating factors – On 26 January 2016 the chairman of the CNIL sent a formal notice to Facebook Inc. and Facebook Ireland to comply with the Data Protection Act. Neither provided any satisfactory answers or remedial action.

Enforcement action – Further to the formal notice dated 26 January 2016, a sanction procedure has been brought against Facebook Inc. and Facebook Ireland. The CNIL pronounced financial claim penalty of 150,000 euros jointly against both companies.

Regulator comment – The CNIL highlighted the significant number of breaches and their particular seriousness but also emphasized that the rights of nearly 33 million of users were infringed.

Observations – The CNIL's decision was subject to an appeal by the two companies before the French administrative Supreme Court ('Conseil d'Etat').

Ongoing investigations

Genesis Industries Limited (China)

Commenced: [date]

Industry – General Business

Incident – This incident relates to connected products, especially children's toys, which are equipped with microphone and loudspeaker associated to a mobile application.

CNIL's investigations revealed that personal information related to children was collected by the Chinese company.

Regulator comment – The CNIL stated that the data processing was not compliant with French data protection laws notably regarding (i) security requirements and (ii) lack of prior information of data subjects.

On 20 November 2017, the chairman of the CNIL sent a formal notice to the Company to comply with the Data Protection Act.

Observations – These proceedings are ongoing. The CNIL currently focuses on the risks of connected objects regarding security and privacy.

Other key developments

Enforcement trends – The CNIL initiated its new strategy in the light of the GDPR by performing in-depth investigations using the full range of control procedures available; on-site, online checks, on documents and auditions.

Sector focus – Insurances and Marketing (especially data brokers).

Litigation

Legal overview

Claims that may be brought by individuals – In France claims can be brought under data protection laws, data privacy and breach of confidentiality.

These causes of action:

- Can be brought before French Courts;
- Apply jointly for enforcing a data protection breach; and
- Lead to administrative, civil and criminal penalties.

Key questions

What is the largest award of damages to date?

To our knowledge one of the largest award of damages was of 15,000 euros (breach of privacy/image rights)

Can damages be obtained for non-financial loss?

Yes, damages can be obtained for non-financial loss in order to compensate non-material damages.

Can claimants bring class actions?

Yes, claimants can bring class actions.

Have they been used for data protection claims? No

Are 'no-win-no-fee' arrangements available? No

Is third party litigation funding available? No

What are the barriers (or perceived barriers) to litigation?

Barriers to litigation may relate to the provision of sufficient evidence to establish a breach regarding data protection.

Notable cases

Claimant(s): Anne P. as known as 'LOUANE'

Defendant(s): SNC Hachette Filipacchi Associes

Industry – Media

Causes of action – Breach of image rights and invasion of privacy.

Significant points of law – Freedom of information was not applicable to images taken from a public individual.

Judgment – The French Court of Appeal ('Cour d'Appel') confirmed the judgment rendered by the French High Court ('Tribunal de Grande Instance').

The Court of Appeal condemned HACHETTE FILIPACCHI ASSOCIES for invasion of privacy and image rights.

Damages – 10,000 euros

Legal costs – 5,000 euros

Other key developments

Media interest – Media show growing interest in all issues relating to personal data. Media covered intensively the GDPR and its consequences especially as regards the latest data breaches such as the 'Cambridge Analytica' scandal involving Facebook security policy.



Pauline Darnand

+33 (38) 84 53 261

pauline.darnand@pwcavocats.com



Michael Chan

+33 3 90 40 26 13

michael.chan@pwcavocats.com

Germany

Data Protection (Directive 95/46/EC)

National law – the Federal Data Protection Act ('BDSG') has implemented the EU Data Protection Directive in Germany.

Regulator – Data protection in the private sector is regulated by the data protection authorities of the German states alongside the Federal Commissioner for Data Protection and Freedom of Information for the federal government.

Enforcement powers – Pecuniary fines or imprisonment of up to 2 years or a fine depending on the severity of the offence.

Penalties –

Law – Maximum fines of EUR 300,000 per violation. The fine shall exceed the financial benefit the perpetrator derived from the administrative offence. If the amounts are not sufficient to do so, they may be increased.

Imposed – A EUR 1.5 million fine was imposed on the Lidl Group for using private detectives and secret cameras in their German shops.

Breach notification – Sec. 42a of BDSG includes a mandatory breach notification, if: sensitive personal data, personal data subject to professional secrecy, personal data related to criminal offences, administrative offences, the suspicion of punishable actions or administrative offences, or personal data concerning bank or credit card accounts has been unlawfully transferred or otherwise unlawfully revealed to third parties, with the threat of serious harm to the data subject's rights or legitimate interests.

GDPR update

The Data Protection Adaption and Implementation Act (DSAnpUG-EU) leads to a new version of the Federal Data Protection Act, which will come in force the day the GDPR comes in force.

The data protection authorities of the German states and the Federal Commissioner for Data Protection and Freedom of Information for the federal government will continue to regulate the newly enacted Data Protection Adaption and Implementation Act.

E-Privacy (Directive 2002/58/EC)

The E-Privacy Directive has been partly implemented in several acts, such as the Telemedia Act (Telemediengesetz) and the Telecommunications Act (Telekommunikationsgesetz), however, the EU has imposed fines on Germany, because the Directive has not as yet been fully implemented.

NIS (Directive 2016/1148)

The NIS Implementation Law of April 2017, leads to a new version of the Act on the Federal Office for Information Security. To some extent, NIS has been implemented in the already enacted German IT Security Act.

Federal legislation is enforced by the Federal Office for Information Security.

Sector-specific regulation

The Telemedia Act

The Telemedia Act (Telemediengesetz) contains sector-specific data protection provisions, which apply to electronic information and communication services except pure telecommunication and broadcasting e.g. web shops, mobile commerce, internet search engines, and company websites.

The regulatory bodies are the same for the Telemedia Act as for BDSG. They monitor implementation of the BDSG and other data protection provisions, with the power to apply pecuniary fines where appropriate.

The maximum fine under the Telemedia Act is EUR 50,000 – with the added requirement that the fine exceed the financial benefit to the perpetrator derived from the administrative offence. If the maximum amounts are not sufficient, they may be increased on a case by case basis.

Section 15a of the Telemedia Act echoes the mandatory breach notification from section 42a of Federal Data Protection Act (FDPA).

The Telecommunications Act

The Telecommunications Act contains sector-specific data protection provisions that apply to telecommunication service providers such as internet access providers.

Section 109a of Telecommunications Act defines the Federal Net Agency and the Federal Commissioner for Data Protection and Freedom of Information as supervisory authorities and provides powers to impose pecuniary fines or imprisonment terms of up to two years for a breach of the act. A limit is placed on fines of EUR 500,000, with the added requirement that the fine exceed the perpetrator's gain, allowing the maximum to be increased where it is not sufficient.

Section 109a Telecommunications Act requires providers of publicly available telecommunications services to notify relevant parties where a breach has occurred.

2017 notable issues

Notable enforcement action/investigations concluded

Debekä

Date of enforcement: December 2014

Industry – Insurance Group.

Incident – Lack of internal controls and violation of data protection law in relation to the purchase of personal data from government employees as potential customers.

Enforcement action – Commissioner for Data Protection and Freedom of Information of the German state Rhineland-Palatinate imposed a fine of EUR 1,300,000.

Litigation

Legal overview

Claims that may be brought by individuals – In Germany, a violation of data protection is reported to the regulatory authority. The data subject usually does not take any actions himself/herself, so that no complaints are regularly filed directly by the data subject.

Notable cases

Claimant(s): Credit Information Agency

Defendant(s): State Data Protection Officer of Baden-Württemberg

Causes of action – The state data protection commissioner of Baden-Württemberg had issued an order against a credit information agency based on the grounds that future violations against the GDPR were already foreseeable. The commissioner argued that according to Section 38 para.2 sentence 1 of the FDPA the supervisory authority can take necessary measures to ensure compliance with data protection provisions in terms of collection, processing and utilisation of personal data.

Mitigating/aggravating factors – This was the first German decision regarding the GDPR.

Judgment – The court confirmed that in case of particularly sensitive data the data protection authority may render order even before the unlawful processing operation if the breach is clearly anticipated. However, in this case such situation was not at hand. In addition the data protection authorities are not entitled to render decisions based on the GDPR before it applies effectively from 25 May 2018.

Claimant(s): Consumer Protection Agency North Rhine-Westphalia

Defendant(s): Fashion ID GmbH & Co. KG belonging to Peek&Cloppenburg KG

Industry – Retail and manufacture

Causes of action – Facebooks 'Like'-Button was embedded on the company website. This meant that data was immediately transferred to Facebook in the USA without the user being able to object to this in advance.

Judgment – The case is still pending before the Court of Second Instance. The Higher Regional Court of Düsseldorf has submitted six questions for referral to the European Court of Justice on this case.

The first instance has ruled that embedding the 'Like'-button on websites violates privacy policy.

Observations – The company has now changed over to a two-click solution. Social media content must now be explicitly activated.



Jan-Peter Ohrtmann

Partner

+49 (0)21 1981 2572

jan-peter.ohrtmann@de.pwc.com

Gibraltar

National law

National law – The Data Protection Act 2004 governs how organisations (both private and public) should use information about individuals.

Regulator – Under the Data Protection Act 2004, the Gibraltar Regulatory Authority (“GRA”) is nominated as the Data Protection Commissioner.

Enforcement powers – Amongst other things, these mechanisms include the provision of advice on data protection related matters and the investigation of complaints, as well as raising awareness on privacy issues.

Penalties –

Law: A fine not exceeding level 5 on the standard scale of fines for offences, this means a maximum amount of £10,000.

Breach notification – Only for some organizations now.

2017 notable issues

Litigation

Legal overview

Claims that may be brought by individuals – In Gibraltar claims can be brought under data protection laws, breach of confidence, misuse of private information, defamation, harassment and employment laws. Unsuccessful litigants may be awarded adverse costs.

Can damages be obtained for non-financial loss?	Yes
Can claimants bring class actions?	Yes
Are “no-win-no-fee” arrangements available?	Yes
Is third party litigation funding available?	Yes
What are the barriers (or perceived barriers) to litigation?	None

Other key developments

Sector-specific campaigns – The GRA has been developing awareness on the GDPR. The GRA has been issuing a series of guidance notes to explain the similarities with the existing Data Protection Act 2004 and describes some of the new and different requirements. It has also taken part in many trainings presented by different organizational bodies across different industries to raise awareness of this new regulation before its commencement date.

A campaign for schools has progressively developed to establish a yearly awareness raising framework involving middle and comprehensive schools in Gibraltar. In this respect, members of the GRA attend the schools to deliver presentations to students, followed by a Q&A session. Students are also asked to complete a privacy survey.

Enforcement trends – The latest notable trends have been all about GDPR.

Sector focus – Due to the size of the financial sector in Gibraltar, the GRA has been involved in developing awareness in industries for this sector.

Guidance – GRA has published multiple articles on GDPR and its introduction.

Legislative and regulatory changes – With GDPR new improvements in this area will come into force.



Isabel Tellez
+35 200 73520
isabel.tellez@gi.pwc.com

Hungary

Data Protection (Directive 95/46/EC)

National Law – The Information Act 2011 ('Act CXII of 2011').

Regulator – Hungarian National Authority for Data Protection and Freedom of Information.

Enforcement powers – The most important enforcement powers/mechanisms are the following. Where the authority establishes an infringement it has the right to:

- initiate judicial procedure; and
- impose financial penalties.

Penalties –

Law – HUF 20.000.000 (equal to EUR 64.000).

Imposed – HUF 20.000.000 (equal to EUR 64.000).

Breach notification – No, it is not mandatory.

GDPR update

Nation law – The legislator intends to modify the Act CXII of 2011 to implement the GDPR regulations and to ensure enforcement. However, the draft of the amendment is not available yet.

Regulator – The Hungarian legislator has not named the supervisory authority yet. It is likely to be the Hungarian National Authority for Data Protection and Freedom of Information.

E-Privacy (Directive 2002/58/EC)

National law – Hungary has implemented the E-Privacy Directive.

Regulator – The regulator is the National Media and Infocommunications Authority.

Enforcement powers – The most important enforcement powers/mechanisms are the following. In cases where the authority establishes an infringement of the Electronic Communication Act (Act C of 2003), has occurred it has the right to:

- initiate judicial procedure;
- impose financial penalties;
- suspend the activity of the company; and
- prohibit the activity of the company.

Penalties –

Law – The amount of the penalty differs depending on the type of the infringement. In some cases the amount of the penalty will be a certain percentage of the company's income. As such it is not possible to determine the maximum financial penalties.

Breach notification – Breach notification is not mandatory

2017 notable issues

Breakdown of enforcement action

Type	No.
Monetary Penalty Notice (i.e. fines)	10
Undertakings	36
Enforcement notices	No information
Prosecutions	No information
Other	No information

Notable enforcement action/investigations concluded

Auchan Magyarország Kft.

Date of enforcement: January 2018.

Industry – Other.

Incident – The incident occurred in connection with illegal electronic surveillance.

Enforcement action – The authority imposed a monetary penalty of HUF 15.000.000 (equal to EUR 48.100).

Regulator comment – The authority determined the legal circumstances/background of the electronic surveillance.

Csodanő Webáruház Korlátolt Felelősségű Társaság

Date of enforcement: July 2017.

Industry – Online technology and telecoms and Marketing.

Incident – The incident occurred in connection with web-shopping and the use of cookies and newsletters.

Enforcement action – The authority established certain undertakings (e.g. stopping the infringement).

Regulator comment – The authority determined the legal circumstances of the use of cookies, newsletters and the legal background of web-shops.

Litigation

Legal overview

Claims that may be brought by individuals – The data subject is allowed to bring a claim against a data controller if the data controller has infringed the rights of the data subjects defined in the Information Act.

These claims aim to gain reimbursement for the damages (financial and non-financial) that occurred to data subject. Most of these claims result in the total reimbursement of the damages, however we have no information about the exact success-rate.

Key questions

What is the largest award of damages to date?

There is no limit.

Can damages be obtained for non-financial loss? Yes

Can claimants bring class actions? Yes

Have they been used for data protection claims? Yes

Are 'no-win-no-fee' arrangements available? Yes

Have they been used for data protection claims? Yes

Is third party litigation funding available? Yes

Has it been used for data protection claims? Yes



Dr. László Réti
Partner of the Law Firm
00361 461 9888
laszlo.reti@pwc.com

Ireland

Data Protection (Directive 95/46/EC)

National Law – The data protection regime in Ireland confers rights to individuals in relation to their personal data, and regulates the collection, processing, storage, use and disclosure of personal data by Data Controllers and Data Processors.

- The Data Protection Acts 1998 and 2003.
- The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (also referred to as the e-Privacy Regulations).
- Ireland is a signatory to the 1980 Organisation for Economic Co-operation and Development ('OECD') Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data as well as the European Convention on Human Rights and Fundamental Freedoms. The Charter of Fundamental Rights of the European Union also applies within Ireland.
- Post 25 May 2018, the General Data Protection Regulation ('GDPR') and Data Protection Act 2018 will apply.

Regulator – The Data Protection Commissioner ('DPC') is tasked with the responsibility of ensuring that the rights of individuals are respected and that those in control of, or processing, personal data adhere to their obligations.

Enforcement powers – The DPC has the power to:

- Undertake investigations, inspections and audits;
- Obtain information required to fulfil its functions;
- Enforce compliance with regulations, which may involve requiring a Data Controller or Data Processor to stop processing data for certain purposes;
- Exercise the powers of an Authorised Officer such as entering premises and inspecting equipment; and
- The DPC also undertakes other activities to identify data protection risks and enhance awareness of, and adherence with, data protection regulations. This may include publishing guidance, consulting with Data Controllers and Data Processors and taking part in speaking events.

Penalties –

Law – The DPC does not currently have powers to directly impose fines. This is expected to change post implementation of the GDPR, which will mean administrative fines can be imposed directly by DPC on the Data Controllers and Data Processors that infringe the regulation (subject to a right of appeal via the Courts).

Imposed – As per the Data Protection Acts, summary legal proceedings may be brought via the Courts. The maximum fine on summary conviction is €3,000. For conviction on indictment, the maximum fine is €100,000.

As per the e-Privacy Regulations, the maximum fine on summary conviction is €5,000 (per communication). For conviction on indictment, maximum fines range from €50,000 for individuals to €250,000 for a body corporate.

Breach notification – Statutory Instrument Number 336 of 2011 sets out the mandatory requirements related to the notification of data breaches by telecommunications providers and internet providers. Under this regulation, providers must notify the competent national authority no later than 24 hours after identifying a breach.

A non-binding 'Personal Data Security Breach Code of Practice' has also been published by the DPC that sets out data breach guidelines.

GDPR update

Once the GDPR comes into effect, it will become mandatory for Data Controllers to notify the DPC of personal data breaches (unless the breach will not result in a risk to the affected data subjects).

2017 notable issues

Notable cases/ongoing investigations

Yahoo (investigation expected to be finalised in early 2018)

Incident – Massive data breach.

Regulator comment – As set out in the DPC 2017 Annual Report 'A central aspect of that investigation concerns the extent to which the **EMEA** controller (Yahoo! EMEA in Dublin) complied with its obligations to ensure that the processing of EU users' personal data by its processor, Yahoo! Inc. was sufficiently secure in terms of technical and organisational measures to safeguard the data'.

Observations – Given the increasingly sophisticated threats to data security (including the advanced technologies being employed by hackers) it is important for organisations to prioritise data protection and to develop comprehensive plans that will enable them to respond effectively to any future breaches. This will become increasingly important under GDPR, where Data Controllers will have an obligation to report breaches within 72 hours (unless there is not a risk to affected data subjects).

Sector-specific campaigns:

Target of campaign – GDPR Awareness Campaign that includes broad guidance as well as guidance tailored for specific sectors, including micro-enterprises

Description of action taken:

- Production of guidance material;
- Speaking events; and
- Media campaigns.

Other key developments

Enforcement trends – Based on the case studies included in DPC's 2017 Annual Report, there was a trend toward Data Controllers and Data Processors complying with recommendations set out by the DPC thereby negating the need to impose enforcement actions.

Sector focus – DPC's organisational structure reflects a focus across all sectors including:

- The public sector and health sector;
- The private sector and financial sector; and
- Multinational and technology sectors.

Given that the DPC will become the lead supervisory authority for many large multinational technology and social network companies post GDPR, there is likely to be a growing focus on engagement with this sector. As indicated in the 2017 DPC Annual Report, recruitment of specialist resources with expertise in emerging technologies will also be prioritised.

Litigation

Legal overview

Claims that may be brought by individuals – Where an individual suffers damage through the mishandling of their personal information, they may be entitled to claim compensation through the Courts. The Data Protection Acts make it clear that where organisations hold personal data they owe a duty of care to those individuals.

While existing processes are in place, the GDPR will further clarify the rights of individuals to claim compensation where there has been a breach of their rights.

Key questions

Can damages be obtained for non-financial loss?

Under the GDPR, compensation may be sought for material and non-material damage. This includes damages that are of a non-financial nature.

Can claimants bring class actions?

There is no provision for class actions in Irish law. ‘Test cases’ and ‘representative actions’ do however operate as forms of class/collective actions.

Are ‘no-win-no-fee’ arrangements available?

Certain firms may offer ‘no-win-no-fee’ arrangements.

Is third party litigation funding available?

There is a system of legal aid available in Ireland for civil law and criminal law (via the Legal Aid Board). There is also a non-state body called the Free Legal Advice Centre (**FLAC**) that offers free legal advice.

What are the barriers (or perceived barriers) to litigation?

The potentially high cost to take court action is a likely barrier to litigation. While legal aid is available, not everyone is eligible, and difficulties may be faced by individuals funding court action privately.

Other key developments

Legislative and regulatory changes – Article 82 of the GDPR states that any person that has suffered either material or non-material damage as a result of an infringement shall have the right to receive compensation from the Data Controller or Data Processor for the damage suffered. Given the expanded obligations under GDPR as well as the enhanced rights of individuals, the number of court proceedings by Data Subjects exercising their rights to compensation is likely to increase.

It will be important for Data Controllers and Data Processors to ensure they have the processes, capabilities and capacity to participate in, and effectively respond to, Court proceedings post GDPR.

Media interest – There is currently high media interest in the area of data protection. This may have been accentuated by recent high profile personal data breaches.

Guidance – DPC maintains regulatory guidance on its website. Ahead of GDPR, additional guidance is likely to become available on DPC’s new website. Guidance is also published by the Article 29 Working Party, which comprises of representatives from the European Union Data Protection Authorities. In particular, recent guidance has been published on ‘Personal Data Breach Notifications’.



Pat Moran

Partner, Cyber Security Lead
+353 (0)8638 03738
pat.moran@ie.pwc.com

Data Protection (Directive 95/46/EC)

National Law – Law no. 675 of December 31, 1996 (the ‘Italian Privacy Code’). This implemented the EU Privacy Directive. It was later abrogated by Legislative Decree no. 196 of 30 June 2003.

Regulator – The Garante (Autorità Garante per la protezione dei dati personali) (‘DPA’). It has offices in Piazza Monte Citorio no. 121, 00186, Rome.

Enforcement powers – In order to verify that processing of personal data is compliant the DPA may:

- order data controllers or processors to adopt specific measures;
- prohibit unlawful or unfair data processing operations, in whole or in part; and
- block processing activities carried out in violation of the law.

It also has general powers to:

- Inquire and control;
- Request information and documents;
- Access databases and filing systems;
- Perform audits at the data controllers’ premises; and
- Carry out investigation.

As a result of the above activities the DPA may also apply sanctions.

Penalties –

Law: Criminal sanctions can be applied in the event of non-compliance with the Italian Privacy Code (secs. 161 and following). Administrative fines currently range from €1,000 to 180,000. The amount charged can vary significantly across cases depending on the level of severity and the existence of any aggravating or mitigating circumstances.

- Failure to notify a personal data breach to the Data Protection Authority (or late notification) shall be punished by an administrative penalty consisting in payment of between €25,000 and €150,000 (sec. 162, Italian Data Protection Code (as modified by Legislative Decree no. 69 of May 28, 2012)).
- Failure to notify a personal data breach to the contracting party or another individual (or late notification) shall be punished by an administrative penalty consisting in payment of between €150 and €1,000 per contracting party or individual concerned. In this case, the ultimate amount of the pecuniary penalty may not exceed 5% of turnover in the applicable accounting year. The amount may nevertheless be increased by up to four times if the pecuniary penalty is found to be ineffective because of the infringer’s financial status.
- Any breach of the provision concerning the obligation to keep an updated inventory of personal data breach shall be punished by an administrative penalty between €20,000 and €120,000 (sec. 162, para. 4, Italian Privacy Code).
- For declaring or attesting to untrue information or circumstances, or submitting forged records or documents, in connection with DPA notifications following a personal data breach, the penalty is imprisonment for between 6 months and 3 years, unless the offence is more serious (sec. 168, Italian Privacy Code).

Imposed – The largest penalty to date was an administrative fine of €11m issued by the DPA in 2017 against five companies operating in the money transfer industry. This was for the unlawful processing of the personal data of around 1000 people.

According to the public available information, it seems that no financial penalties have been applied by the Italian Data Protection Authority for failure in data breach notifications.

Breach notification – providers of publicly available electronic communication services must notify the Garante without undue delay of any personal data breach (sec. 32, Italian Privacy Code).

GDPR update

Italy is still awaiting the issuance of the legislation which will coordinate the GDPR with the provisions included in the Italian Privacy Code.

Post-GDPR the regulator for the processing of personal data under the GDPR will still be the Garante.

E-Privacy (Directive 2002/58/EC)

This was implemented in Italy by the Italian Privacy Code.

NIS (Directive 2016/1148)

The Italian Legislative Decree implementing the NIS Directive was approved by the Italian Government on 8 February 2018. It is currently in the process of being issued by the Italian Head of State.

According to the press release issued by the Italian Government the regulators responsible for the enforcement of the NIS Directive have been identified. At the time of the drafting of this paper, the regulators have not yet been disclosed.

Sector-specific regulations

- Electronic communications industry: new rules regarding security breaches for this sector.

These were implemented alongside other amendments to the Italian Privacy Code by Legislative Decree no. 69 of May 28, 2012. The legislation introduced the definition of personal data breach, as well as the obligation for publicly available electronic communications services to notify the DPA of the breach of any personal data they hold.

Following on from this the Garante issued Guidelines (4th April 2013) on the implementation of measures for notify personal data breaches. These clarified the circumstances under which a provider is required to notify personal data breaches, as well as the format applying to such notification.

The DPA later issued further Guidelines (12 November 2014; 4 June 2015) regarding notification of breaches relating to biometric and medial patient data (within the electronic patient dossier: dossier sanitario).

- Financial institutions are bound by a specific obligation imposed by the Bank of Italy (circular no. 285 of 17 December 2013) to report to the Bank of Italy or to the Central Bank of Europe any serious breach of information security.

2017 notable issues

In June 2018 the DPA's Annual Report is expected to be published, summarizing decisions taken over the previous year. Ahead of this publication the material below provides a general overview based on the publicly available information.

Breakdown of enforcement action

Type	Value
Monetary Penalty Notices (i.e. fines)	€1.7m ²

² Total amount of fees collected as of the first semester of 2017.

Industry	Number of fines	Highest fine	Total value
Charitable and voluntary	–	–	–
Criminal justice	–	–	–
Education and childcare	3	40,000	74,000
Finance insurance and credit	5	5,880,000	11,010,000
General business	–	–	–
Health	11	20,000	158,000
Land or property services	–	–	–
Legal	1	4,000	4,000
Local government	9	100,000	250,000
Marketing	19	64,000	530,000
Media	–	–	–
Online technology and telecoms	6	60,000	230,000
Other (gaming)	1	20,000	20,000
Political	–	–	–
Retail and manufacture	1	20,000	20,000
Transport and leisure	6	40,000	126,000
Total	62	6,248,000	12,422,000

Notable enforcement action/investigations concluded

Sigue Global Limited

Date of enforcement: 2 February, 2017

Industry – Finance, insurance and credit.

Incident – operating together with four others in the money transfer sector, the company registered the names of individuals in the centralized archive required by AML laws without their prior consent.

This was done in order to hide the identity of the people who were sending money and thereby avoid reaching thresholds set by AML legislation.

Mitigating/aggravating factors – The unlawful processing was carried out with respect to a database of significant size (around 1000 individuals). The DPA considered the unlawful processing of personal data of each individual as a standalone violation, with a consequent increase in the sanctions applied.

Enforcement action – considering the aggravating factors described above, the DPA applied an administrative fine of an overall amount of €11m.

Regulator comment – further comments from the DPA will probably be made available in the Annual Report to be published in June.

Observations – this was a milestone decision for the DPA, also in the light of the higher sanctions introduced by the GDPR which will be applicable from May of 2018.

Other key developments

Sector focus – according to the DPA October 2017 newsletter the focus for the second semester of 2017 included personal data processed by, or within:

- Call center operators (especially if located in Albania);
- IT system of the Italian National Institute of Statistics; and
- Local health companies requested by multinational companies operating in the pharmaceutical industry.

Litigation

Legal overview

Claims that may be brought by individuals – With respect to data protection/privacy, in Italy claims can be brought in the following areas:

- Data protection laws;
- Breach of contract (confidentiality clause);
- Employment laws;
- Defamation;
- Harassment; and
- Persecuting behavior (i.e. stalking).

The actions brought under Privacy Code (D. Lgs. 196/2003) are not aimed at restoring damages suffered by individuals. Therefore such restorative claims shall be brought by the data subject under article 2043 of the Italian Civil Code.

Key questions –

Can damages be obtained for non-financial loss?

Yes, Article 2059 of the Italian Civil Code allows indemnification also for damages not related to financial losses (i.e. danno non patrimoniale).

Can claimants bring class actions?

Class actions under Italian law are regulated by Article 140 of the Italian Consumer Code.

Have they been used for data protection claims?

According to local news, in December 2017 a class action was launched against a Municipality in Italy for the illegal publication on its website of the personal data of citizens who did not pay fines inflicted for the violation of traffic laws. The amount requested was of €700,000.

Are ‘no-win-no-fee’ arrangements available?

No. In the Italian legal system lawyers are bound by obligations only with respects to the means used for the performance of their duties (i.e. ‘obbligazione di mezzi’) and not also with respect to results (i.e. ‘obbligazione di risultato’). Therefore, such arrangements are not used.

Is third party litigation funding available?

No

What are the barriers (or perceived barriers) to litigation?

The most important deterrent to litigation in Italy is the extended length of the trials, which may last for years.

Other key developments

Sector-specific campaigns – Target of campaign – During the first semester of 2017 the main private sector targets of DPA investigations were:

- Credit or financial intermediation;
- Credit collection;
- Offering of home sales; or
- Commercial information services;
- Sharing economy;
- Dental centers; and
- Phone marketing.

With respect to the public sector, investigation activities mainly focused on the application of security measures and audit systems.

Activities performed during the first semester of 2017 resulted in the application of more than 300 sanctions and 20 reporting to the Judicial Authority for criminal violations.

Media interest – the media is interested in enforcement actions taken with respect to the protection of personal data, especially considering the current era of digital innovation and the imminent application of the GDPR.

Privacy groups/lobbyists – various conventions and conferences on GDPR have been organized by the main Italian privacy groups and associations (e.g. Federprivacy).



Andrea Lensi
+39 06 57178538
andrea.lensi@pwc.com



Stefano Cancarini
+39 02 91605212
stefano.cancarini@pwc.com



Flavia Messina
+39 02 91605054
flavia.messina@pwc.com

Liechtenstein

Data Protection (Directive 95/46/EC)

National law – Liechtenstein enacted the Data Protection Act on 14th of March 2002 ('DPA'). This implemented the EU Data Protection Directive.

Regulator – Federal State Parliament.

Enforcement powers – The Data Protection Office, which is organisationally assigned to the Federal State Parliament, supervises the compliance of public authorities with the DPA and is allowed to make recommendations. If these recommendations are not followed, the Data Protection Office can submit the case to the Data Protection Commission for a decision. A sanctions system allows for fines or prison sentences to be imposed in the case of a violation of the DPA.

Penalties –

Law – Financial penalties up to 360 daily rates or imprisonment up to one year.

Breach notification – The DPA contains no mandatory breach notification. It's on a voluntary basis, if the Data Protection Office investigates a data protection breach or if a private data protection officer reports a data breach.

GDPR update

For the implementation of the GDPR and especially of the opening clauses, the DPA is currently in a revision process. The consultation procedure was completed on the 28th of February 2018. Entry in force is planned at the beginning of 2019. The focus of the revision process is as mentioned on the implementation of the opening clauses of the GDPR. The independence of the supervisory authority is strengthened and the organisational assignment of the Data Protection Office is changed to the Ministry of Justice. The international cooperation between supervisory authorities is strengthened as well as the penal provisions to satisfy the requirements of the GDPR.

Regulator – The regulator will continue to be the Federal State Parliament.

E-Privacy (Directive 2002/58/EC)

The EEA Joint Committee adopted the E-Privacy Directive on 20th of June 2003 to the EEA Agreement. The requirements of the E-Privacy Directive are implemented by the Communication Act.

Regulator – The regulator will continue to be the Federal State Parliament. It has a sanctions system which includes punishments up to three months in prison or monetary sanctions up to 180 daily rates.

There is no mandatory breach notification requirement.

Sector-specific regulation

Protection of privacy mentioned in the Civil Code.

Communication Act: The operator has a duty to notify a breach if an implemented phone number is used in an abusive way.

Communication Act: If a phone number is used in an abusive way, the owner has a right to claim compensation.

Regulator – The Federal State Parliament has a sanctions systems where monetary penalties can be imposed.

Under the Communication Act, breach notifications of abusive use of phone numbers are mandatory.

2017 notable issues

Notable enforcement action/investigations concluded

Data Protection Office

Date of enforcement: September 2017

Industry – All industries.

Incident – The Data Protection Office has published a recommendation with regard to the elimination process of personal data. They recommend to destroy personal data instead of just deleting them. This provides more security for that personal data can't be recovered after deletion. This view is also in accordance with the GDPR. Companies which follow this recommendation would be in compliance with the GDPR.

Mitigating/aggravating factors – Simple deletion of data is often not sufficient to remove the information completely because technical tools are able to recover them.

Enforcement action – The Data Protection Office has published the recommendation regarding destruction of personal data.

Regulator comment – Because the revised Data Protection Act contains both terms for eliminating persona data (destroy and delete), it is up to the processor which mechanism will be followed. With regard to the requirement of the GDPR, it is recommendable to destroy data completely.

Ongoing investigations

Telecommunication firm

Industry – Online technology and telecoms

Incident – A telecommunication firm has made a study on the purchasing behavior of customers. For this reason, they have recorded and analyzed the movements of the customer's smartphones. According to the telecommunication company, the data were anonymized.

Mitigating/aggravating factors – The Data Protection Office launched an investigation into the case. The focus of the investigation lies on the fact, if the data were correctly anonymized or not. The investigation will be completed during the year 2018.

Litigation

Legal overview

Claims that may be brought by individuals

- Right of information;
- Claim for blocking data transfers; and
- Claim for deletion of personal data.

The DPA contains also penal provisions: Violation in the duty of information or cooperation and violations of data secrecy.

It is also possible to bring in a claim based on the Civil Code in respect of a violation of personal rights.

Claims are also possible based on the Penal Code.

Key questions

Can damages be obtained for non-financial loss?

It's possible to claim for non-financial damages in form of a satisfaction because of the suffered harm.

Are 'no-win-no-fee' arrangements available?

No

What are the barriers (or perceived barriers) to litigation?

Barriers are as usual the high court costs connected with the risk of losing a case.

Notable cases

Claimant(s): Higher Administrative Court of Sweden/
Court of Appeal

Defendant(s): European Court of Justice (preliminary
ruling procedure)

Industry – Other

Causes of action – The question submitted to the European Court of Justice was if national regulations for general retention of data through telecommunication firms are allowed.

Mitigating/aggravating factors – Retention of data means systematic storage of phone and internet data of natural persons without any suspicion to a crime.

Significant points of law – The most significant point of law was if national regulations for general retention of data violates fundamental individual rights. The judgment is important for Liechtenstein, because the fundamental rights of the EU Charter are comparable with the fundamental rights of Liechtenstein.

Judgment – The European Court of Justice decided that EU member states are only allowed to retention of data when a strong connection to a severe punishment is presumed. National regulations for general retention of data violate fundamental rights.

Ongoing investigations

Claimant(s): Data Protection Office

Defendant(s): Telecommunication firm

Industry – Online technology and telecoms

Causes of action – A telecommunication firm has made a study on the purchasing behavior of customers. For this reason, they have recorded and analyzed the movements of the customer's smartphones. According to the telecommunication firm, the data were anonymized.

Mitigating/aggravating factors – The Data Protection Office launched an investigation into the case. The focus of the investigation lies on the point, if data were correctly anonymized or not. The investigation will be completed during the year 2018.

Significant points of law – See above

Other key developments

Media interest – wide ranging application has generated considerable media interest.



Susanne Hofmann-Hafner
+41 58 792 17 12
susanne.hofmann@ch.pwc.com

Netherlands

Data Protection (Directive 95/46/EC)

National Law – Directive 95/46/EC has been published in the Official Journal of the European Union on 23 November 1995. The Directive has been implemented through the Personal Data Protection Act that came into effect on September 2001.

Regulator – The Dutch Data Protection Authority ('DPA') (*Autoriteit Persoonsgegevens*) supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data. The most important laws are the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*), the Police Data Act (*Wet politiegegevens*) and the Basic Registration of Persons Act (*Wet basisregistratie personen*).

Enforcement powers – Upon violation of the provisions, the Dutch DPA may impose an administrative penalty. The administrative penalty shall not exceed the amount of the sixth category of article 23, paragraph 4 of the Criminal Code. If there is a violation of the Dutch DPA, which has been committed intentionally or was the result of serious culpable negligence, the supervisory authority may immediately impose an administrative penalty. If there is no case of a violation of the Dutch DPA, a binding instruction will precede the imposition of an administrative penalty.

Penalties –

Law – In case of violation of the data breach notification obligation, the Dutch DPA may impose an administrative penalty. The maximum amount of the penalty is € 820,000. For a telecom company that does not report on a data breach, the maximum penalty is € 900,000.

Imposed – No administrative penalty has ever been imposed.

Breach notification – On 1 January 2016, the data breach notification obligation has come into force.

Regulator – The Dutch Financial Authority ('AFM') and Dutch DPA when it comes to data breaches. This mandatory notification only exists if a data breach is also an incident. In the case of such a breach, it must be reported to Dutch National Bank ('DNB') and to the Dutch DPA who enforce an administrative penalty.

The maximum financial penalties can be up to € 820,000.

A data breach must be notified to the supervisory authority. There is a mandatory breach notification, but not on the grounds of the Personal Data Protection Act. This mandatory breach notification corresponds to the duty of care of FS organizations.

GDPR update

An Implementation Act is being designed by the Dutch government. This draft meets the need left to the Member States to enforce the GDPR.

The Dutch DPA supervises processing of personal data in order to ensure compliance with the GDPR.

E-Privacy (Directive 2002/58/EC)

Directive 2002/58/EG will be replaced by the e-privacy regulation, simultaneously (as a *lex specialis*) with the GDPR. In the Netherlands, the EPR is implemented in the Telecommunications Act 1984 ('Telecommunicatiewet').

Regulator – Until 1 January 2016, the Authority for Consumers and Markets ('ACM') was the regulator when it came to data breaches. As of 1 January 2016, notifications will be made to the AP (in the case of security breaches). The ACM remains competent with regard to the other violations of the Telecommunications Act 1984 whose enforcement powers are:

- Imposing administrative sanctions, such as a penalty and an order for incremental penalty payments.

In case of violation of the mandatory notification for data breaches, the Dutch DPA or the ACM may impose an administrative penalty. The maximum amount of the penalty is € 900,000 or up to 10 percent of annual worldwide revenue for failure to comply with the directive.

A mandatory breach notification is in place and providers of public electronic communication services and networks have an obligation to report to the ACM (and a duty to report to those involved). When it concerns a data breach the reporting obligation may also fall under the Data Protection Act.

NIS (Directive 2016/1148)

Last status: an opinion of the Raad van State (Dutch Advisory body on legislation and administrative court) was issued on 4 January 2018. The transposition of the NIS Directive into national law shall take place no later than 9 May 2018.

Regulator – It is reasonable to expect the DNB will serve as supervisor.

Sector-specific regulation

An exception to the obligation to report a data breach to the data subject is made for financial institutions as referred to in the Financial Supervision Act ('FSA'). If a financial institution notifies the parties concerned, they do so based on their obligation as a financial institution.

2017 notable issues

Break-down of enforcement action

In the first (135), second (123) and third (245) quarter of 2017 written warnings have been given to controllers and processors of personal data by the Dutch DPA. No number of written warnings over the fourth quarter 2017 was available.

Notable enforcement action/investigations concluded: – In 2017 several investigations by the Dutch DPA to processors of data were announced in the Dutch media. No enforcement actions have been taken so far.

Notable enforcement action/investigations concluded

Uber B.V.

Date of enforcement: November 2017

Industry – Transport and leisure

Incident – Uber paid hackers who stole personal data, then kept the data breach quiet. No report was made to the Dutch DPA and the data breach was not communicated to the people concerned. Uber recognizes after the publication of this news that it has encountered a hack.

Regulator comment – A taskforce, led by the Dutch DPA and composed at this stage of representatives from the Belgian, German, French, Italian, Dutch and Spanish DPAs as well as from the ICO, will coordinate the national investigations of the various DPAs on the Uber data breach case.

Observations – The Dutch DPA is currently investigating this data breach notification. No concrete results are available yet.

Other key developments

Enforcement trends – The question has been raised whether the regulator immediately should impose penalties. The corporate world started a (modest) lobby to maintain the information task of the Dutch DPA for a longer time and to take enforcement action to a lesser extent.

Litigation

Legal overview

Claims that may be brought by individuals – Claims can be brought under Wrongful act under the Dutch Civil Code, Dutch Data Protection Act, the Police Data Act and the Basic Registration of Persons Act

Concerns have the power to bring actions before national courts. It is not a standard legal practice so far. This attitude could change with the introduction of the GDPR.

Key questions

Can damages be obtained for non-financial loss?

Damages can be obtained for non-financial loss.

Can claimants bring class actions?

It is possible. However, to our knowledge no class actions by claimants were applicable.

Is third party litigation funding available?

No litigation funding by third parties has been occurred.

What are the barriers (or perceived barriers) to litigation?

No barriers are perceived.

Other key developments

Sector-specific campaigns – A campaign on privacy by the government, in anticipation of the GDPR, is active in the Netherlands since 29 January 2018.

This campaign is aimed at citizens and government.

Guidance – The Policy rules for the application of article 34a under the Dutch Data Protection Act are still in charge.



Yvette van Gernerden

+31(0)88 792 54 42

+31(0)652 00 59 24

yvette.van.gernerden@nl.pwc.com

Poland

Data Protection (Directive 95/46/EC)

Regulator – General Inspector for Personal Data Protection ('GIODO')

Enforcement powers – GIODO has the power to:

- Supervise and ensure data processing is compliant with the provisions on the protection of personal data;
- Issue administrative decisions and consider complaints with respect to the enforcement of the provisions on the protection of personal data;
- Impose financial penalties for non-fulfilment of non-pecuniary obligations arising under the decisions referred to in point above;
- Keep the register of data filing systems and the register of administrators of information security, as well as provide information on the registered data files and the registered administrators of information security;
- Issue opinions on bills and regulations with respect to the protection of personal data;
- Initiate and undertake activities to improve the protection of personal data; and
- Participate in the work of international organisations and institutions involved in personal data protection.

Penalties –

Law – The maximum financial penalty for natural persons is 10,000 zł and the total sum of multiple penalties cannot exceed 50,000 zł.

For legal persons, and organisations with no legal personality but which are granted legal capacity, each penalty cannot exceed 50,000 zł and the total sum of multiple penalties cannot exceed 200,000 zł.

Breach notification – Not mandatory.

GDPR update

National law – The New Personal Data Protection Act will regulate:

- Entities obliged to designate their data protection officers and the procedure for the designation notification;
- Conditions and proceedings related to certification and accreditation;
- Proceedings concerning code of conduct approval;
- Supervisory authority (i.e. President of the Office of Personal Data Protection);
- Rules concerning the format and procedures applicable to the notification of personal data breaches;
- European administrative cooperation;
- Supervisory measures;
- Civil liability for data protection breaches; and
- Administrative penalties for data protection breaches.

Regulator – President of the Office of Personal Data Protection ('PUODO').

E-Privacy (Directive 2002/58/EC)

National law – Poland has implemented the Directive.

Regulator – GIODO and President of the Office of Electronic Communication (President of UKE).

Enforcement powers – In addition to the above mentioned powers, when it comes to the providers of publicly available electronic communications services, GIODO can:

- order the service provider to communicate a personal data breach to the data subjects; and
- supervise compliance with informational duties and the maintenance of the inventory of personal data breaches.

Furthermore, in the scope of the personal data protection, President of UKE has the power to impose penalties in case of non-compliance with the informational or notification duties incumbent on providers of publicly available electronic communications services.

Penalties –

Law – Up to 3% of an entity's revenue from the previous calendar year. Additionally, a natural person who manages the undertaking can be fined with a penalty of up to 300% of his or her monthly salary. Please note that these competences only apply to the President of the UKE.

Breach notification – Mandatory breach notification. This is applicable to the providers of publicly available electronic communications services.

NIS (Directive 2016/1148)

Nation law – Currently, the National Cyber Security System Act, which will implement the NIS Directive, is in the advanced stage of the legislative process.

Regulator

- Government Representative for the Cyber Security alongside with Collegium for the Cyber Security; and
- Minister in charge of digitization (in general) and other respective ministers (accordingly to their scopes of responsibilities provided in aforementioned act).

2017 notable issues

Breakdown of enforcement action

Type	No.
Undertakings	199
Enforcement notices	64
Prosecutions	45
Complaints filed with GIODO	2,690

Notable enforcement action/investigations concluded

Ministry of Digitization

Date of enforcement: 12 September 2017
(upheld 9 November 2017)

Incident – The GIODO discovered that the Ministry of Digitization, as a controller of data included in the Universal Electronic System for Registration of the Population (PESEL) register, had violated the data protection regulations by:

- lacking security procedures in case of personal data breach incidents;
- granting single users with more than one certified card which provides access to the PESEL register;
- lacking functionality in the user application which would indicate the basis for the data processing; and
- not implementing software for system logs analysis (including operations performed by a user with granted access).

Mitigating/aggravating factors – During the case, the ministry updated its certification policy to make it impossible to grant a single user with more than one access card to the PESEL register.

Enforcement action – The General Inspector for Personal Data Protection ordered the Ministry of Digitization to:

- develop and implement security procedures in case of personal data breach incidents;
- modify the user application to enable the indication of the basis for the data processing; and
- implement system logs analysis software.

Regulator comment – According to the regulator, the aforementioned irregularities are a serious threat for the data security of Polish citizens. The users of the PESEL register (mostly bailiffs) were granted excessive and uncontrolled access to the vast amount of personal data without having to provide the basis for their data processing. Furthermore, due to lack of system logs analysis the ministry, as the data controller, was unable to control the purpose of data enquiries.

Observations – The regulator's actions should be evaluated positively as it raised public awareness of data protection issues.

Other key developments

Enforcement trends – Several now-defunct private universities are under investigation by the regulator due to a potential breach of personal data protection. These institutions allegedly abandoned students' documentation in the buildings they used to operate in and did not take proper measures to protect the data. The controllers, formally active yet no longer operating, oftentimes could not be reached. As result, the regulator reported the offences to the prosecutor. The investigation is still ongoing.

Litigation

Legal overview

Claims that may be brought by individuals

- Personal interest infringement actions; and
- Delict action.

Personal interests, such as one's personal data, are protected by civil law independent of the protection envisaged in other provisions:

- The person whose personal interests are threatened by another person's activity may demand the omission of that action, unless it is not illegal. In case of an infringement, he may demand that the person who committed the infringement perform acts necessary to nullify its effects and in particular to make a statement of the appropriate contents and in an appropriate form.
- In the case of an infringement of one's personal interests, the court may award pecuniary compensation to a person whose personal interests have been infringed. This will be for an appropriate amount as pecuniary compensation for the wrong suffered.
- The data subject may also claim for the redress of damage caused by delict.

Key questions

Can damages be obtained for non-financial loss?	Yes
---	-----

Can claimants bring class actions?

Yes, but only in delict actions.

Have they been used for data protection claims?	Not yet
---	---------

Are 'no-win-no-fee' arrangements available?	No
---	----

Is third party litigation funding available?

It's permitted under the freedom of contracts rule but it's not widely used.

What are the barriers (or perceived barriers) to litigation?

Low public awareness of the importance of data protection. The incoming GDPR that is coming into the force is supposed to change that matter for better.

Notable cases

Claimant(s): Unidentified

Defendant(s): Telecoms Company

Industry – Online technology and telecoms

Causes of action – Personal interest infringement

Significant points of law – The professional telecommunication services provider, as a data controller, is culpable of a data breach if he misuses client's trust by entrusting a third party with processing duties without the client's consent.

The Polish Data Protection Act provisions are meant to be treated as *lex specialis* to the general 'fault in the choice' rule in the Polish Civil Code when it comes to the professional telecommunication services providers that subcontract the processors. As a consequence, such controllers cannot exculpate themselves using the general rule in case of a processor's data breach. As a result, the controller should select the processors with enhanced due diligence.

Judgment – In favour of claimant. The appealed verdict was set aside in whole and the case was remanded to the court which issued the verdict. The process is still ongoing and there is no publicly available. More information will be available upon the awarded damages.

Other key developments

Media interest – Readiness for GDPR, aspects of data protection in new technologies and social media.



Gerard Karp
+48 502 184 707
gerard.karp@pwc.com



Mateusz Fuchs
+48 519 506 599
mateusz.fuchs@pwc.com

Portugal

Data protection (Directive 95/46/EC)

National law – In Portugal, you have to consider the following main laws:

- Portuguese constitution;
- 1995 European Directive for Data Protection. This was transposed into law in 1998;
- Health: Personal information on genetics;
- Electronic communications: retention periods, database of 'bad payers';
- Direct marketing law;
- Surveillance: means of surveillance of private and public security companies;
- Labour: Privacy on the labour code;
- Citizen card: National Identification document; and
- Cybercrime law.

The Portuguese legal framework for Data Protection is not very demanding. The current law is from 1998, and the Data Protection Authority does not have capacity to respond to requests concerning this law in a timely manner. Therefore, there are considerable number of unanswered requests.

Additionally, a very low number of privacy violations are registered or even 'publicised' in the media. This suggests that the Portuguese market is not aware of this subject but, even if it does value it, significant emphasis will be required in order for it to be considered a valid focus.

Regulator – Comissão Nacional de Proteção de Dados.

Enforcement powers – Analysis of requests from companies to process certain types of personal data, and have the power to approve it or identify changes to implement in order to be approved.

Penalties imposed – A telecommunications company was fined €600,000 when a collaborator passed personal information to a third party for espionage purposes.



Jorge Sacadura Costa
+351 914 142 752
jorge.sacadura.costa@pt.pwc.com

Romania

Data Protection (Directive 95/46/EC)

National law – Law 677/2001 regarding the protection of persons in relation to the processing and circulation of personal data. This implements Directive 95/46/EC.

Regulator – National Supervisory Authority for Personal Data ('NSAPD').

Enforcement powers – NSAPD reports infringements and sets sanctions.

Penalties imposed – The largest penalty to date was for EUR 75,000 (equivalent to RON 340,000). The maximum financial penalty under Law 677/2001 is RON 500,000.

Breach notification – Law 677/2001 does not specify any mandatory requirements to report data breaches.

GDPR update

NSAPD has issued guidelines on the application of the GDPR.

E-Privacy (Directive 2002/58/EC)

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector has been implemented by Law 506/2004 regarding the processing of personal data and the protection of privacy in the electronic communications sector.

The NSAPD is the regulator for the E-Privacy Directive.

The maximum financial penalty provided amounts to RON 100,000 or, in the case of an undertaking with a turnover more than RON 5,000, up to 2% of the turnover.

NIS (Directive 2016/1148)

The law has been drafted to implement the NIS Directive, due to come into force on 9 May 2018. The regulator for this law will be the Romanian National Computer Security Incident Response Team.

Sector-specific regulation

Data breach is also regulated by the National Authority for Management and Regulation in Communications ('NAMRC'), pursuant to the Emergency Ordinance no. 111/2011 regarding electronic communications.

NAMRC produces statement-of-facts detailing contraventions along with the sanction to be applied pursuant to a written resolution by the NAMRC's president.

2017 notable issues

Breakdown of enforcement action

Type	No.
Monetary Penalty Notice (i.e. fines)	193 fines
Undertakings	357

Industry	Number of fines	Total value (RON)
Finance insurance and credit	23	382,000
Local government	13	29,500
Total	193	1,008,500

Notable enforcement action/investigations concluded

ERB Retail Services IFN S.A.

Date of enforcement: November 2016

Industry – Finance insurance and credit

Incident – illegal processing of personal data. ERB Retail Services IFN S.A. did not handle the requests of the data subjects (6 petitioners) exercising the right of intervention, namely to adopt measures for the deletion of negative data transmitted to the Credit Bureau, without their prior notification.

Enforcement action – Sanctions totaling RON 42,000 were applied.

Other key developments

Enforcement trends – NSAPD's approach is to primarily apply sanctions consisting of warnings (as per statistics provided in their activity report of 2016).

Litigation

Notable cases

Claimant(s): Mr. Bogdan Mihai Bărbulescu

Defendant(s): The Romanian Government

Industry – Other

Causes of action – Dismissal by the employer based on the breach of the right to respect for private life and correspondence (Violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms), which provides:

- 'Everyone has the right to respect for his private and family life, his home and his correspondence; and
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Significant points of law – The Court specifies the criteria to be applied by the national authorities when assessing whether a given measure is proportionate to the aim pursued and whether the employee concerned is protected against arbitrariness. In particular, the authorities should determine the following:

- Whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures;
- The extent of the monitoring by the employer and the degree of intrusion into the employee's privacy;
- Whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content;
- Whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications;
- The consequences of the monitoring for the employee concerned and the use made by the employer of the results of the monitoring operation; and
- Whether the employee has been provided with adequate safeguards, especially when the employer's monitoring operations are of an intrusive nature.

Judgment – The Court concluded that, in reviewing the decision of Mr Bărbulescu's employer to dismiss him after having monitored his electronic communications, failed to strike a fair balance between the interests at stake: namely Mr Bărbulescu's right to respect for his private life and correspondence, on the one hand, and his employer's right to take measures in order to ensure the smooth running of the company, on the other.

The Court concluded that Mr Bărbulescu's right to respect for his private life and correspondence under Article 8 was not adequately protected by the national authorities.

Damages – Mr. Bărbulescu claimed EUR 59,976.12 in respect of the pecuniary damage he had allegedly sustained. The Court did not discern any causal link between the violation found and the pecuniary damage alleged, and therefore dismissed this claim.

Mr. Bărbulescu claimed EUR 200,000 in respect of the non-pecuniary damage he had allegedly sustained as a result of his dismissal. The Court considered that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicant.

With regard to cost and expenses The Court considered reasonable to award the applicant the sum of EUR 1,365 covering costs under all heads.

Other key developments

Legislative and regulatory changes – The draft law on measures to implement the GDPR covers new aspects, such as the processing of the national identification number (which includes personal identification number, the serial and number of the identity document, passport number, driving license number and health insurance social number). Such processing must be within the legitimate interests of the data controller or a third party and may only be undertaken if the data controller has established the following safeguards: (i) implementing technical and organisational measures to comply with data minimisation and security and confidentiality of data processing, (ii) the appointment of a Data Protection Officer, (iii) the adherence to a code of conduct, (iv) the establishment of a specific storage terms and circumstances when data must be deleted or revised, (v) detail the obligations of those who process personal data under direct authority of the data controller or data processor.

Media interest – Media interest is high in this field.

Guidance – NSAPD recommends the appointment of a Data Protection Officer although in some cases it is not necessary to have a designated individual.



Bianca Naghi
+40748201644
bianca.naghi@david-baias.ro



Daniel Vinerean
+40742588127
daniel.vinerean@david-baias.ro



Corina Badiceanu
+40742526231
corina.badiceanu@david-baias.ro

Switzerland

National law

National law – Data protection in Switzerland is regulated by the Swiss Federal Data Protection Act of 1992 ('FDPA') which is currently under revision.

The Data-Protection-Directive 95/46/EC is not applicable in Switzerland.

Regulator – Federal Data Protection and Information Commissioner ('FDPIC').

Enforcement powers – The FDPIC is able to give recommendations to companies. A sanctions system allows it to also impose fines in case of a violation of the FDPA. Sanctions can be issued against responsible natural persons within the company only and not against the company itself as a legal person.

Penalties –

Law – The maximum financial penalty under FDPA is 10,000 Swiss Francs.

Breach notification – Not currently mandatory.

GDPR update

On the first hand, companies will be responsible to take account of whether they fall under the scope of the General Data Protection Regulation ('GDPR'), especially considering the extraterritorial scope of the GDPR (Art.3 (2)). Simultaneously and also in order to satisfy the requirements of the GDPR, the FDPA is in a revision process. Data protection and the individual rights of citizens are strengthened. Further, administrative powers for the FDPIC are introduced. A mandatory notification system of data protection breaches is implemented and fines in case of privacy violations are increased to a new maximum of 250,000 Swiss Francs. The revised FDPA is meant to adjust data protection in Switzerland to a level equal to the European standard which makes data exchanges within the EU (and the EEA) easier. The revised Swiss Federal Data Protection Act is expected to come in force at the beginning of 2019.

E-Privacy (Directive 2002/58/EC)

The E-Privacy Directive has not been implemented but developments in the EU are being monitored.

NIS (Directive 2016/1148)

It remains to be seen if legislative modifications for Switzerland due to the implementation of the NIS Directive in the EU member states will be necessary. Certain regulations of the NIS Directive are fulfilled already. Switzerland has adopted a National strategy for the protection of Switzerland against Cyber-risks ('NCS'). Switzerland also has a working Computer Emergency Response Team ('CERT') and keeps a list of critical sectors and partial sectors.

The Federal IT Steering Unit ('FITSU') is the responsible Unit in the Federal Administration and is also monitoring the situation.

Sector-specific regulation

Labor Law: Art. 328 of the Swiss Code of Obligations. The duty of care of the employer requires that an employee needs to be informed if there is an unauthorized access to their personal data.

Providers of telecommunication services: Disturbances in the network need to be reported to the Federal Office of Communications ('BAKOM') if a relevant number of customers are affected (Art. 96 of the Swiss Telecommunications Law).

2017 notable issues

Breakdown of enforcement action

Ongoing investigations

Swiss telecommunication provider

Industry – Online technology and telecoms

Incident – On the 7 February 2018, the Swiss telecommunication provider reported to the FDPIC unauthorized access by third parties to private contact details of around 800,000 customers. Those mainly affected are private mobile accounts and some fixed-line network customers.

Regulator comment – The FDPIC requested the company in application of Art. 29 Abs. 2 FDPA to take position. First investigations have shown that a causal link between the unauthorized accesses cannot be softened. The FDPIC continues to collect more information for a risk evaluation.

Observations – Theft of data is a very present risk. For this reason, appropriate security measures need to be focused too.

Enforcement trends – During the discussions of the introduction of the GDPR and also with regard to the revision process of the Swiss Federal Data Protection Act there were intentions of a 'Swiss Finish' for the new data protection system. The idea was, to get the Swiss data protection standard to a higher level than the EU. This approach will not be followed because of economic reasons.

Litigation

Legal overview

Claims that may be brought by individuals Art. 12 Abs. 2 FDPA provides a list of actions, which lead to a breach of privacy; there are 9 actions listed as possible claims for a breach of privacy.

The FDPA contains also penal provisions; violation in the duty of information or cooperation (Art. 34 FDPA), and violations of professional secrecy (Art. 35 FDPA). In the revised Swiss Federal Data Protection Act, claims for breaches in duty of care (Art. 55 E-DSG) will also be possible.

It is also possible to bring a claim based on the Swiss Civil Code if there is a violation of personal rights (Art. 28 of the Swiss Civil Code).

Claims based on the Swiss Code of Obligations are possible for damage-reparation (Art. 41 CO). Data breaches through the employer are stated in Art. 328b CO.

Claims are also possible based on the Swiss Penal Code (e.g. Art. 179 – 179, Art. 162 SPC etc.).

Claims based on the penal provisions in the Swiss Federal Data Protection Act have small practical relevance, because the subjective matter requires deliberate intention. The advantage of a claim based on the Swiss Federal Data Protection Act and also on the Swiss Civil Code compared to the GDPR is that the Swiss Legal System allows claims for data protection violation against every natural person, which influences data processing in a company (not just against the data protection officer or the operator of the job).

Claims based on the Swiss Code of Obligations are very rare. It appears to be rather difficult to evidence to a damage due to a breach of privacy.

Key questions

Can damages be obtained for non-financial loss?

It is possible to claim for non-financial damages if harm has been suffered.

Can claimants bring class actions?

Class actions are not possible, but it is possible to bring an action on behalf of several members of an association.

Have they been used for data protection claims?	Yes
--	-----

Are 'no-win-no-fee' arrangements available?	No
--	----

What are the barriers (or perceived barriers) to litigation?

Barriers are the high court costs connected with the risk of losing a case.

Notable cases

Claimant(s): FDPI officer

Defendant(s): Not named

Industry – Other

Causes of action – Provider did not accept the recommendation of the Federal Data Protection and Information Officer. For this reason, the FDPI complained to the Federal Administrative Court.

Significant points of law – One issue was deciding whether personality profiles transmitted by the provider especially in connection with information for solvency analyses, fall in the scope of the Swiss Federal Data Protection Act. Another issue was the listing of this data in search engines.

Judgment – The Swiss Federal Administrative Court came to the conclusion that the definition of a personality profile is independent of whether the data is publicly available or not. The origin of the data source is irrelevant for the definition of a personality profile. For this reason, a justification for the transmission of data profiles is needed. The Swiss Federal Administrative Court qualifies search engine listing as transparency supportive. The provider is not obliged to support faster cancellations of search engine listing. The Swiss Federal Administrative Court also decided that the provider has to check the accuracy of the database.

Other key developments

Sector-specific campaigns – Suppliers of digital campaigns for political reasons – This campaign targets suppliers of digital applications, e.g. political groups or associations. These applications are used for interactions with specific groups of persons. Algorithmic tools allow the inserted data from those applications to be connected to the political interests of a person. The FDPIC decided that in application of Art. 4 Abs. 5 FDPA, data processing in those applications are only allowed if the relevant person explicitly allowed the processing.

Guidance – With regard to the revision of the Swiss Federal Data Protection Act and also the entry of the GDPR, the revised Swiss Federal Data Protection Act encourages the establishing of codes of conduct. Trade associations and other economic interest groups can submit these codes of conduct for consideration to the FDPIC. These codes of conduct will not have any legal significance. Nevertheless, it will have impacts on the self-regulation of the companies.



Susanne Hofmann
+41 58 792 17 12
susanne.hofmann@ch.pwc.com



International Trends – Rest of World

- 1. Argentina*
- 2. Australia*
- 3. Canada*
- 4. China*
- 5. Georgia*
- 6. India*
- 7. Japan*
- 8. Mauritius*
- 9. Mexico*
- 10. New Zealand*
- 11. Paraguay*
- 12. Peru*
- 13. Russia*
- 14. South Africa*
- 15. Turkey*
- 16. UAE*
- 17. USA*

Total

17

Argentina

National law

National Law – Argentine Data Protection Law No. 25,326

Regulator – Argentine Data Protection Agency (“Dirección Nacional de Protección de Datos Personales”)

Enforcement powers – Law 25,326 establishes the obligation of database owners and data users to register all databases designed to provide information to third parties in a special registry managed by the Argentine Data Protection Agency.

The Argentine Data Protection Agency has the power to issue regulations applicable to the protection of data and to impose sanctions on those who do not comply with them.

Specifically, the Argentine Data Protection Agency is entitled to:

- assist individuals on the data protection regulations and on the legal remedies available to defend their rights;
- conduct a census on data files, registers, or data banks governed by the law 25,326 and maintain a permanent record of them;
- control the observance of the rules on integrity and data security by the data files, registers or data banks. For this purpose, the Agency may request judicial authorization to access premises, equipment, or data processing programs in order to verify any infringement to the law;
- request information from State-owned and/or private entities, which must provide the background, documents, programs or other elements related to the processing of personal data. In these cases, the Agency must guarantee the security and confidentiality of the information and elements being provided;
- impose applicable administrative sanctions for any infringement to the law and its regulations;
- be a plaintiff in any criminal actions that are initiated for violations of this law; and
- supervise the compliance of the legal requirements and guarantees that private data files or data banks must meet in order to provide reports.

In addition, the Argentine Criminal Code considers as a criminal offence the willful processing of false personal data and the breach of confidentiality or of data security.

Section 117 (b) of the Code provides for one month to two years’ imprisonment for any person who knowingly inserts or orders to insert false information in a personal data file. The punishment shall be from six months to three years for any person who knowingly provides a third party with false information obtained from a data file. The maximum and the minimum term of the punishment shall each be increased by one half when the deed results to the detriment of any person. Finally, when the perpetrator or person liable for the crime is a public official holding office, an additional penalty applies consisting in a ban to hold any public office for a period of time that shall double that of the conviction.

Section 157 (b) of the Code provides for imprisonment penalties from one month to two years for (a) any person who knowingly and unlawfully, or in violation of confidentiality and security data systems, obtains information from a personal data file in any way, and (b) any person who reveals to another information registered in a personal data file which, pursuant to law, he or she is obliged to maintain confidential. If the author is a public official, limited disqualification to hold public office from one to four years shall also be imposed.

Penalties –

Law – The Law provide for administrative sanctions and penalties.

Administrative sanctions may be imposed by the Data Protection Agency and consist of warnings; suspension; fines from Ar\$1,000 (approximately US\$50) to Ar\$100,000 (approximately US\$5,000); and closure of the database.

There are however maximum limits to the application of sanctions to the same offender. For mild offences, such limit is of Ar\$ 1,000,000 (approx. USD 50,000); for serious offenses is of Ar\$3,000,000 (approx. USD 150,000) and for very serious offences is of Ar\$5,000,000 (approx. USD 250,000).

The penalties shall apply to the responsible persons or users of public or private data banks, bases, registries or records designed to provide information, either registered or not at the pertaining registry, notwithstanding the administrative liability of responsible persons or users of public data banks, or the civil liability derived from violations to the Personal Data Protection Law and other applicable criminal penalties.

The application and the graduation of the administrative sanctions shall be assessed according to the nature of the affected personal rights, the quantity of data being treated, the benefit gained, the intent of the author, whether the breach is a second offense, the damages and losses caused to the interested party and/or any other third parties, and any other circumstance relevant in assessing a particular offense.

Imposed: The largest penalty to date has been Ar\$3,000,000 (approximately USD 250,000), resulting from an aggregate of 1 mild offense and 268 serious offenses.

Breach notification: Not mandatory.

Law 25,326 establishes the obligation of database owners and data users to register all databases designed to provide information to third parties in a special registry managed by the Argentine Data Protection Agency.

2017 notable issues

Notable enforcement action/investigations concluded

Advance Development Solutions S.R.L.

Defendant(s): Google

Industry – Financial, insurance and credit

Incident – This local credit rating company was providing personal information exceeding the credit records of individuals.

Mitigating/aggravating factors – None.

Enforcement action – Fine of Ar\$60,000.

Regulator comment – The regulator indicated what type of information exceeded from the one needed to evaluate the financial condition of an individual.

Observations – Credit rating companies started to be carefully supervised as from then, especially regarding the sort of information that they provide through their websites.

Other key developments

Without necessarily amounting to a trend, over the past year Argentine Data Protection Agency activities have focused on financial services, lending and credit rating companies.

The Argentine Data Protection Agency has not issued any regulatory guidance, and there has not been any significant publicity or media interest in the Argentine Data Protection Agency's enforcement actions.

Litigation

Legal overview

Claims that may be brought by individuals

In Argentina, claims may be brought on the following grounds:

- habeas data;
- the right to privacy established in the Civil and Commercial Code;
- employment laws; and
- criminal actions.

Habeas data is a constitutional right designed to protect data privacy by giving access to the courts. It is a judicial action that any person may file to obtain information about themselves, the purpose for which such data was stored, and for amending, updating or eliminating incorrect data.

Right to privacy is reinforced by Section 53 of the Civil and Commercial Code which requires the personal data owner's consent for the reproduction or publication of an image or voice, but also for the capturing thereof.

Employment Contract Law No. 20,744 principles require that the dignity and privacy of employees must be respected. Good faith must be observed by employers and employees according to the Labor Contract Law.

Correspondence, including emails and their traffic information are confidential. There are currently two opposing positions or trends disputing whether the employer is legally allowed to monitor work emails of its employees.

Most criminal and labor court decisions rendered until today consider corporate electronic communications as a work tool and apply, in the absence of specific regulations, the general labor framework, with the consequent powers of control for the employer. The other position equates emails to any other written communication or correspondence, protected by the constitutional right to privacy, where no monitoring is allowed.

A recent decision of division I of the Criminal Court of Appeals followed this trend and considered that the employer had no right to scan employees' emails (Criminal Court of the City of Buenos Aires, Division I, in re "G., R. S. and others. Action seeking nullity and costs" – Docket file No. 41.816/2014, Decision of Feb 13, 2015).

The Court of Appeals ruled that employee emails presented by the employer were inadmissible evidence in a criminal complaint, even if the employee had been warned that his/her communications could be monitored during the course of his/her employment.

The Court of Appeals considered that once an employee is given a user and personal access password to the company's server/system, all communications become constitutionally protected private correspondence.

The Court of Appeals disregarded the company policy warning that all communications could be monitored by corporate management and stated that employees' consent to this type of policies are not free and spontaneous, and therefore insufficient to waive their right to privacy. According to this precedent, employer email revisions would require a specific, ad hoc consent by the employee.

Criminal actions – Cybercrime Law No. 26,388, which amended the Criminal Code, penalizes with imprisonment of one month to one year the person who illegally opens or accesses an electronic communication, letter, correspondence, etc., not addressed to him/her. It also penalizes anyone who intercepts electronic communications or telecommunications coming from private systems or of restricted access.

Key questions

Can damages be obtained for non-financial loss?	Yes
Can claimants bring class actions?	Yes
If so, have they been used for data protection claims?	Yes
Are 'no-win-no-fee' arrangements available?	Yes
If so, have they been used for data protection claims?	Yes
Is third party litigation funding available?	No
What are the barriers (or perceived barriers) to litigation?	
One important barrier is given by the time it takes a case to be decided upon. Normally, the resolution of a case may take up to more than five years of litigation (i.e. lower and appeal courts)	

Notable cases

Claimant(s): Belén Rodríguez

Defendant(s): Google

Industry – Online technology and telecoms

Causes of action – The case tackles the issue of the civil liability of web search engines derived from the content listed on their databases.

Mitigating/aggravating factors – The Argentine Supreme Court ruled that Google and other ISPs are not liable for the content of third parties if the ISP does not have knowledge of the allegedly infringing material or, having such knowledge, acts expeditiously to remove access to such material.

Significant points of law – Up to present, Argentina has not enacted any regulation on the liability resulting from different activities on Internet.

Judgment – The Court rejected the petition of the plaintiff to apply the strict objective liability rule established in the Civil and Commercial Code to the search engines. Nevertheless, the Argentine Supreme Court stated that there could be cases when search engines would be held liable such as when they know about the illegality of the content but do not act in a diligent way, which requires the application of the subjective-fault liability rule.

Damages – N/A

Legal costs – N/A

Observations – The Argentine Supreme Court rejected all the petitions of the plaintiff and brought certainty on a very complex legal issue involving ISP liability.

Other key developments

The Argentine Data Protection Agency has drafted a data protection bill, mainly based on the EU GDPR. The main changes to be introduced by the bill –if approved – consist in:

- the elimination of the duty to register databases;
- the recognition of only individuals as data subjects;
- the definition of biometric data and genetic data, amongst other concepts;
- the introduction of new legal bases, other than consent, for data processing, including processing that is in the legitimate interest of the data controller (i.e., with a similar test as the one brought by the GDPR); and
- the overhaul of the current rules of cross border transfers of personal data, including the admission of Binding Corporate Rules as legal basis for data transfers;
- new regulations governing child consent, cloud computer, data breaches, accountability, the duty to have a data protection officer, amongst others.

Local media in Argentina is normally interested in covering the cases involving the civil liability of web search engines derived from the content listed on their databases, especially referring to local politicians, models, actors and other celebrities.

There are NGOs in Argentina that are interested in data privacy matters.



Pedro Luis de la Fuente

+54 11 4850 4733

pedro.de.la.fuente@ar.pwc.com

Australia

National law

National Law – the key privacy law in Australia is the Privacy Act 1988 (Cth) (“Privacy Act”), incorporating the Australian Privacy Principles. The Privacy Act is supported by regulation, industry codes, and Australian State/Territory based law.

Regulator – The Office of the Australian Information Commissioner (“OAIC”).

Enforcement powers – OAIC has the power to:

- assist individuals on the data protection regulations and on the legal remedies available to defend their rights;
- undertake a privacy investigation, whether initiated as a result of a privacy complaint or the Commissioner himself;
- conduct privacy assessments (akin to an audit) of entities;
- make determinations in respect of the above investigations, which may include actions to be taken and/or damages;
- bring proceedings to enforce a determination;
- accept enforceable undertakings from a person or entity;
- bring proceedings to enforce an enforceable undertaking;
- seek an injunction; and
- apply to the court for a civil penalty order.

It is open to the OAIC to use a combination of enforcement powers to address a particular matter.

Penalties –

Law: The maximum financial penalty under the Privacy Act is 2,000 penalty units, or A\$420,000.

Imposed: The largest penalty to date has been \$23,000 for FY17.

Breach notification – From 22 February 2018, mandatory data breach notification will take effect in Australia.

The regime requires agencies and organisations that are regulated by the Privacy Act to notify the OAIC and affected individuals of an ‘eligible data breach’, which occurs where:

- There has been unauthorised access or disclosure of personal information held by an entity which is, a reasonable person would conclude, ‘likely to result in serious harm’ to any of the individuals(s) to whom the information relates; or
- Personal information has been lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur, and if it were to occur, a ‘reasonable person’ would conclude that it is ‘likely to result in serious harm’ to any of the individuals to whom the information relates.

The regulated entity will be required to notify the OAIC and affected individuals as soon as practicable after it is aware, or ought reasonably to have been aware, that there are reasonable grounds to believe that there has been an eligible data breach. If an entity suspects an ‘eligible data breach’, the regime requires that entity to carry out an assessment of whether there are reasonable grounds to believe an ‘eligible data breach’ has occurred’.

Sector-specific regulation

There are three sector-specific privacy codes (the “Codes”) which have been registered in accordance with the Privacy Act. The Codes do not impose sector-specific regulations in respect of a data breach.

- Privacy (Australian Government Agencies – Governance) APP Code 2017, which takes effect on 1 July 2018;
- Privacy (Market and Social Research) Code 2014; and
- Privacy (Credit Reporting) Code 2014 (v1.2).

Legislative and regulatory changes

Several are proposed or will take effect in 2018:

- Notifiable Data Breaches (NDB) scheme, which takes effect on 22 February 2018;
- The extraterritorial impact of the GDPR to those Australian entities who are caught within the scope;
- The Australian Government Agencies Privacy Code, which takes effect from July 2018; and
- The Consumer Data Right, which is proposed to be legislated for certain sectors in 2018.

These changes are unlikely to impact existing claims, however, the notifiable data breaches scheme is intended to ensure regulated entities are more proactive and transparent in handling data breaches. No doubt the OAIC will be seeking to take early enforcement action for non-compliance with the NDB scheme.

2017 notable issues

Breakdown of enforcement action

In Australia, the OAIC typically takes enforcement action via:

- Complaint investigation/conciliation;
- Determinations;
- Enforceable undertakings;
- Commissioner initiated investigation (CII) reports; and
- Privacy Assessments.

Type	No.
Monetary Penalty Notice (i.e. fines)	125
Undertakings	2
Determinations	9
Commissioner-initiated investigations	29
Assessments	10

Notable enforcement action/investigations concluded

Department of Immigration and Border Protection (DIBP)

Commenced: February 2014

Industry – Government

Incident – A Commissioner-initiated investigation was commenced following a media report that a database containing the personal information of approximately 10,000 asylum seekers in immigration detention was available on DIBP's website.

The investigation focused on whether DIBP had reasonable security safeguards in place to protect the information and whether the information had been disclosed in accordance with the Privacy Act.

In November 2014, the Commissioner found that there had been a data breach, made several recommendations for action but was satisfied that the steps that DIBP has and will take in response to the breach will assist DIBP to strengthen its privacy framework and meet its privacy obligations.

Regulator comment – Following a representative complaint made to the OAIC on 30 August 2015, on 24 January 2018, the OAIC issued a statement seeking to contact individuals that were affected by this breach and who believe they have suffered loss or damage as a result of the breach, in advance of the Commissioner making a recommendation in respect of this matter.

Observations – The Commissioner will shortly make determination on this matter under the Privacy Act which will involve whether a remedy, including any compensation, should be awarded to any individual group members who had suffered loss or damage as a result of the data breach.

Department of Health/data.gov.au

Industry – Government

Incident – A Commissioner-initiated investigation was commenced in relation to Medicare Benefits Scheme and Pharmaceutical Benefits Scheme data sets which were published on data.gov.au and subsequently re-identified by academics at a Victorian university.

Regulator comment – On 18 December 2017 the Commissioner noted that it is continuing to work with Australian Government agencies to enhance privacy protection in published data sets; as there is value of public data to innovations that benefit the community at large.

Observations – This was a significant matter which resulted in swift legislative action, with the introduction of a Bill which would make it an offence to re-identify de-identified government data which has been published (the Bill has not yet passed). More information on the Bill can be found in our PwC Legal Talk.

Australian Red Cross Blood Service (Red Cross)

Industry – Charitable and voluntary

Incident – A database file containing information relating to approximately 550,000 prospective blood donors who had entered their details into the website was inadvertently saved to a public-facing web server by an employee of a third-party provider.

Regulator comment – The OAIC found that the Red Cross responded effectively and responsibly to the breach, but nevertheless should have had in place better measures to prevent third party breach.

The root cause of the incident was a one-off human error on the part of a third-party provider's employee. As there was no authorisation or direct involvement by Red Cross, they were not in breach of APP 6.

Nevertheless, there were two matters within the Red Cross' control that were a contributing factor to the data breach and which constituted breaches of the Privacy Act:

- the absence of contractual measures or other reasonable steps on the part of the Red Cross to ensure adequate security measures for personal information held for it by the relevant third party contractor, in breach of APP 11.1
- The retention of data on the Red Cross website for a longer period than was required, in breach of APP 11.2.

Observations – All organisations should consider privacy obligations and implementing sufficient security measures when engaging third-parties, as privacy obligations cannot be outsourced.

Additionally, the Red Cross' proactive action in notifying the OAIC and individuals affected was viewed favourably.

Ongoing investigations

Industry – Transport and Leisure; Health

Uber – Data breach due to hack, exposing 57m users' personal information.

Flight Centre – Alleged data breaches involving the release of personal information of third-party suppliers.

The Cosmetic Institute – Alleged data breach occurred after an error allowed the public to view The Cosmetic Institute's website index which included medical forms and images.

Observations – These investigations are ongoing, and the OAIC is continuing to work with the respective affected companies. Further details are expected at the conclusion of each investigation.

Other key developments

Enforcement trends – The OAIC's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to ensure best privacy practice and prevent privacy breaches.

The factors that the OAIC will take into account in deciding when to take privacy regulatory action, and what action to take. Some of the key factors include:

- The seriousness of the incident or conduct to be investigated (or the potential impact of a proposal), including:
- The number of persons potentially affected;
- Whether the matter involves 'sensitive information' or other information of a sensitive nature;
- The adverse consequences caused or likely to be caused to one or more individuals arising from an incident or conduct;
- Whether disadvantaged or vulnerable groups may have been or may be particularly adversely affected or targeted;
- Whether conduct was deliberate or reckless;
- The seniority and level of experience of the person or persons responsible for the conduct;
- The level of public interest or concern relating to the conduct, proposal or activity;
- Whether the entity responsible for the incident or conduct has been the subject of prior compliance or regulatory enforcement action by the OAIC, and the outcome of that action; and
- Action taken by the entity to remedy and address the consequences of the conduct.

Sector focus – The OAIC is guided by a range of information sources for the purpose of identifying systemic privacy issues. This isn't necessarily a sector-specific focus. Information sources include:

- Individual complaints and data breach notifications;
- Complaint and data breach notification trends;
- International developments;
- Media reports;
- Informants;
- Surveys;
- Privacy assessments;
- Commissioner initiated investigations – credit reporting body annual reports;
- Information from recognised external dispute resolution schemes, including in annual reports provided to the OAIC; and
- Reports from APP code administrators.

Litigation

Legal overview

Claims that may be brought by individuals – A breach of the Privacy Act is considered to be an 'interference with the privacy of an individual'.

The cause of action is an overarching cause of action which applies to any breach of the Privacy Act.

Key questions

<i>Can damages be obtained for non-financial loss?</i>	Yes
<i>Can claimants bring class actions?</i>	Generally a representative action is brought where a number of claimants are affected.
<i>Are 'no-win-no-fee' arrangements available?</i>	This is dependent on the fee terms agreed between lawyer and client.
<i>Is third party litigation funding available?</i>	Possibly, where representative actions are taken.
<i>What are the barriers (or perceived barriers) to litigation?</i>	Australian privacy law is principles based and assessment of whether there has been a breach in the circumstances is not black and white.

Notable cases

Claimant(s): Privacy Commissioner

Defendant(s): Telstra Corporation Ltd

Industry – Online technology and telecoms

Causes of action – Judicial review (of OAIC determination)

Mitigating/aggravating factors – This was a test case brought by the OAIC to seek certainty around the meaning of metadata.

Significant points of law – Whether metadata constitutes ‘personal information’ for the purposes of the Privacy Act 1998 (Cth).

Judgment – Mr Ben Grubb (Grubb) requested all personal information held by Telstra (an Australian telco company) about him, including mobile network metadata such as IP addresses and geolocation data. Telstra refused to hand over such data.

A complaint was made to the Commissioner, who found in favour of Grubb and declared that he was entitled to the information. The Administrative Appeals Tribunal overturned this decision in respect of the metadata, finding that this was information about the service provided by Telstra to Grubb and not about Grubb himself.

The Full Federal Court of Australia found that certain information which is not directly personal information (e.g. such as metadata) can in some circumstances – e.g. when combined or stored with other types of information – constitute personal information; information about an individual. This is an evaluative conclusion depending on the facts of the case.

Legal costs – Applicant to pay the costs of the respondent.

Observations – This is a significant decision in Australian privacy law, but has not resolved the question of when metadata constitutes personal information.

The OAIC has welcomed this decision, writing that it:

“provides important guidance as to what is ‘personal information’ in the terms of the Privacy Act 1988. In particular, the Court has confirmed that assessing what is ‘personal information’ requires an ‘evaluative conclusion, depending on the facts of any individual case’ and that “even if a single piece of information is not ‘about the individual’ it may be about the individual when combined with any other information”. This is consistent with how ‘personal information’ has been interpreted by my office....Obtaining clarity for business and agencies about the definition of personal information was my primary interest in the appeal.”

PwC’s perspective is that although this case confirms that metadata is capable of constituting personal information, further judicial or legislative guidance is required on the test that should be applied.

Other key developments

Sector-specific campaigns – Credit Reporting Information – The Privacy (Credit Reporting) Code 2014 (v1.2) forms an important part of the regulation of credit reporting. PwC was appointed by the Commissioner to undertake an independent review of the Code which was released in December 2017.

Open Data in Banking Sector – The Australian Government recently released its report into the Review of Open Banking. The key recommendation was that banking customers have a right to direct banks to share to other banks, as selected by the customer, all personal information about the customer, free of charge. This excludes ‘value added’ data (i.e. data which the bank has materially enhanced due to insights, analysis or transformation).

Media interest – A big media focus has been the Notifiable Data Breaches scheme in Australia commencing 22 February 2018, which at the date of writing has not yet come into effect.

We expect the implementation and enforcement of this scheme to generate further developments in privacy law in Australia and continue to attract significant media attention.

There was significant legal commentary relating to the Grubb proceedings, as the outcome was not as clear as expected.

Guidance – The OAIC has published a guide to privacy regulatory action, including a dedicated chapter to civil penalties. The maximum civil penalty, for a serious or repeated interference with privacy, is currently A\$420,000.

Privacy groups/lobbies – As a general comment, representative bodies such as consumer groups are quite engaged in relation to proceedings, investigations and reviews.



Tony O'Malley
+61 (2) 8266 3015
tony.omalley@pwc.com



Sylvia Ng
+61 (2) 8266 0335
sylvia.ng@pwc.com

Canada

National law

National Law – In Canada, data protection is governed by a patchwork of laws and regulations, a summary of which is provided below (note: this does not include federal and provincial public sector laws that address privacy and often freedom of information in the public sector).

Personal Information Protection and Electronic Documents Act (“PIPEDA”) governs the commercial use, collection and disclosure of personal information. This applies to private sector organizations and within provincial jurisdictions provided a province has not passed its own law which has been recognized as “substantially similar”. PIPEDA does not apply to employee data unless the sector is a federally regulated business (e.g. banks, telecom). PIPEDA has been recognized as providing an adequate level of protection to personal data by the EU Commission (Commission Decision 2002/2/EC).

Provincial Legislation

- Provinces with privacy legislation deemed “substantially similar” to PIPEDA include the following but note that substantial similarity does not automatically bring a law under Canada’s adequacy finding:
 - Alberta’s Personal Information Act (“AB PIPA”);
 - British Columbia’s Personal Information Protection Act (“BC PIPA”); and
 - Québec’s An Act Representing the Protection of Personal Information in the Private Sector (“PPIPS”).
- Provinces with privacy health privacy laws that have been declared substantially similar to PIPEDA:
 - Ontario – Personal Health Information Protection Act (“ON PHIPA”);
 - New Brunswick – Personal Health Information Privacy and Access Act (“NB PHIPAA”);
 - Newfoundland and Labrador’s – Personal Health Information Act (“NL PHIA”);
 - Nova Scotia – Personal Health Information Act (“NS PHIA”); and
 - Canadian Anti-Spam Legislation (“CASL”) governs electronic communication and provides a regime for commercial electronic messages as well as software installed on users’ devices. The enforcement agency is the Canadian Radio-Telecommunications Commission (“CRTC”). This law is currently subject to review.
- Genetic Anti-Discrimination Act (“GNA”) criminalizes requirements to provide genetic data for obtaining insurance.

Data Localization

- PIPEDA does not prohibit the movement of personal information outside Canada. However, Canadian residents’ data remains subject to PIPEDA;
- British Columbia’s Freedom of Information and Privacy Protection Act prohibits British Columbia residents’ health data from being stored outside Canada;
- Nova Scotia (Personal Information International Disclosure Protection Act) requires public bodies to keep personal information in Canada unless under specific circumstances;
- New Brunswick’s PHIPAA requires consent for transfer of information held by public bodies outside Canada;

- Under Alberta’s PIPA, organizations must notify individuals if their data is being processed outside of Canada;
- Quebec’s law restricts personal information from being exported unless the information is protected to the same extent as under provincial law;
- Note that many public sector departments and agencies prohibit, by contract or policy personal, information from being taken out of Canada. Some private sector organizations also prohibit employee data from being exported due to union requirements;
- Office of the Privacy Commissioner of Canada (“OPC”); provincial legislation is enforced by its respective privacy commissioner or ombudsman; and
- CASL is currently enforced by the CRTC, the OPC and the Competition Bureau (“CB”).

Enforcement powers – The following regulatory enforcement mechanisms are available in Canada:

- Undertakings;
- Investigations/audits;
- Monetary penalties;
- Compliance agreements;
- Mediations;
- Power to summon witnesses, administer oaths and compel the production of evidence; and
- Notice of violations.

Penalties –

Law:

PIPEDA:

- Failure to comply with PIPEDA’s mandatory breach notification obligations could result in fines of up to:
- CAD \$10,000 on summary conviction; and
- CAD \$100,000 on indictment.
- Organizations that contravene PIPEDA may be required to enter into a compliance agreement with the OPC, which could then be enforced by the Federal Court.

On Phipa:

- An individual found guilty of committing an offence under ON PHIPA can be liable for a fine of up to CAN \$100,000, while an organization or institution can be liable for a fine of up to CAN \$500,000.
- If an organization commits an offence under ON PHIPA, every officer, member, employee or agent of that corporation found to have authorized the offence, or who had the authority to prevent the offence from being committed but knowingly refrained from doing so, can also be held personally liable.

CasL:

- The consequences for violating CASL are substantial with a number of companies receiving large penalties. If a company is found to be in violation of CASL, there are a number of enforcement mechanisms available, including:
- A maximum penalty of up to \$1 million for individuals and \$10 million for businesses. However, this can also include other costs, such as legal fees and reputation damage. Directors, officers and agents can also be held personally liable in the event of a violation; and
- A Private Right of Action for CASL has been introduced. However, it has currently been postponed by the Canadian government.

Imposed – The CRTC fined Compu-Finder CAN \$1.1m for spamming potential customers with offers of unsolicited training courses and violating CASL. This fine was recently reduced to \$200,000.

Breach notification:

Federal:

PIPEDA was amended to include mandatory breach notifications to the OPC of a breach of security safeguards. Where the breach poses a “*real risk of significant harm*”, then notification must be made to the individuals affected. The amendment also included mandatory record keeping requirements. This was deferred until a regulation was developed under PIPEDA; the Data Breach Regulation, which addresses the form of notices and content. This is expected to come into force in 2018 or early 2019.

The factors that are relevant to determining whether a breach creates a “real risk of significant harm” to the individual include:

- The sensitivity of the personal information involved in the breach;
- The probability that the personal information has been, is being or will be misused; and,
- Any other prescribed factor.

Provincial:

Organizations subject to AB PIPA are required to notify the OPC when a privacy/security breach results in a “real risk of significant harm” to an individual as a result of the loss or unauthorized access or disclosure of their personal information.

Organizations subject to ON PHIPA are mandated to report privacy breaches, as defined in regulation, to the Information and Privacy Commissioner and, in certain circumstances, to relevant regulatory colleges.

GDPR update

The Canadian legal framework will have to be amended to update them for adequacy under GDPR requirements. Notably, the Federal Commissioner has requested increased enforcement powers, and as noted the Data Breach Regulation will improve equivalence with the GDPR. The ETHI Committee of the Federal Parliament has also recently recommended incorporation of privacy by design into PIPEDA along with other requirements to move more in line with GDPR requirements (e.g. data portability).

Legislative and regulatory changes

The ETHI Parliamentary Committee Report, released February 2018, has recommended a number of substantial changes to PIPEDA including enforcement powers to the OPC, Privacy by Design, a right to be forgotten, and others. This may become the basis for Canada’s “GDPR light.” This is only a set of recommendations at this time and it may or may not lead to legislation. The timing as well is not certain.

2017 notable issues

Breakdown of enforcement action

OPC Statistics from Annual Report April 1, 2016 – March 31, 2017

Type	No.
PIPEDA complaints accepted	325
PIPEDA complaints closed through early resolution	205
PIPEDA complaints closed through standard investigation	89
PIPEDA data breach reports	95
Privacy Act complaints accepted and processed for investigation	1,357
Privacy Act complaints closed through early resolution	423
Privacy Act complaints closed through standard investigation	660
Privacy Act data breach reports	147

Notable enforcement action/investigations concluded

Individual

Date of enforcement: 16 March 2017

Industry – Health

Incident – A Masters of Social Work student was found to have been illegally accessing the records of family, friends, local politicians, staff of the clinic and other individuals in the community. Following an investigation, the matter was further referred to the Attorney General of Ontario for prosecution.

Mitigating/aggravating factors – The individual accessed the personal health information of 139 individuals without authorization between 9 September 2014 and 5 March 2015.

Enforcement action – The individual was ordered to pay a CAN \$20,000 fine and a CAN \$5,000 victim surcharge for accessing personal health information without authorization.

Regulator comment – “*Health care professionals need to know that this kind of behaviour, whether it’s snooping out of curiosity or for personal gain, is completely unacceptable and has serious consequences. This judgement sends a message through Ontario’s health care system that unauthorized access will not be tolerated. Further, there is an obligation to ensure that proper safeguards are in place to prevent this kind of activity. Patient privacy is vital if Ontarians are to have confidence in their health care system.*”

Observations – This is the highest fine to date for a health privacy breach in Canada. It sets a standard for regulators when addressing health records snooping cases.

Other key developments

Enforcement trends – Canadian privacy commissioners are paying close attention to the health industry and snooping.

Canadian privacy commissioners will also be looking at all industries to enforce mandatory breach notification once the regulations come into force.

The OPC is looking at a pure consent driven approach thereby limiting the circumstances where businesses can innovate with data without consent.

Canada is expected to see a more proactive approach for enforcement by the regulators, particularly in matters relating to consent and access to personal information. This may occur for two reasons:

- The OPC powers may need to match those in the EU so Canada can achieve adequacy status under the impending General Data Protection Regulation (GDPR); and/or
- The OPC is open to enabling use of data without consent by businesses for broader societal purposes and data driven innovation contingent on, and you guessed it, enhanced OPC powers.

Sector focus – Mandatory breach notification will span across a number of sectors.

Litigation

Legal overview

Claims that may be brought by individuals – Privacy laws in Canada do not generally give private rights of action. One exception was CASL but note that the coming into force of this right was deferred by the Government of Canada pending a review of CASL.

Civil actions for the tort of invasion of privacy or intrusion upon seclusion are being recognized in the common law courts of Canada (Jones v. Tsige).

Manitoba's The Intimate Image Protection Act creates a private right of action for non-consensual sharing of intimate images.

Nova Scotia's Cyber-Safety Act created a right of action, which was subsequently struck down as unconstitutional (Crouch v Snell) under the Canadian Charter of Rights & Freedoms.

Development of these cases is fairly recent, therefore there are not many such cases.

Key questions

What is the largest award of damages to date?

Damages range from CAN \$4100 to CAN \$10,000 in cases involving intrusion upon seclusion. In one case concerning the publication of intimate images, which was subsequently set aside (Jane Doe 464533) to permit the defendant to set aside default and file a defence; damages were initially awarded for CAN \$100,000.

Can damages be obtained for non-financial loss?	Yes
--	-----

Can claimants bring class actions?	Yes
---	-----

Is third party litigation funding available?
Possibly, where representative actions are taken.

Have they been used for data protection claims?

At this point, certification proceedings have been begun for claims made arising from violations of ON PHIPA (Hopkins v Kay).

Are “no-win-no-fee” arrangements available?

Not generally, under most provincial class proceedings certifications laws, arrangements are subject to court review.

Is third party litigation funding available?

Application can be made under some provinces' laws for funding.

Has it been used for data protection claims?

Not at this time.

Notable cases

Equifax Inc.

Industry – Finance, insurance and credit

Incident – Equifax experienced a privacy breach that also implicated Canadians.

Regulator comment – The OPC has opened an investigation into the data breach at Equifax Inc. after receiving several complaints and dozens of calls from concerned Canadians.

Observations – The results of the investigations will provide further clarity into the breach and the follow up actions taken by Equifax Inc.

Nissan Canada

Industry – Transport and leisure

Incident – Nissan has indicated that the exact number of people affected by the breach is not known, but that it was contacting more than 1.1 million current and past customers who financed their vehicles through Nissan Canada Finance and Infiniti Financial Services Canada.

Regulator comment – The OPC has opened an investigation into the data breach at Nissan Canada Finance.

Observations – The results of the investigations will provide further clarity into the breach and the follow up actions taken by Nissan.

Claimant(s): Jones

Defendant(s): Tsige

Industry – Finance

Causes of action – Tort for intrusion upon seclusion.

Significant points of law – Recognition of tort of intrusion upon seclusion in Ontario.

Judgment – Awarded damages of CAN \$10,000.

Observations – Precedent setting and potentially dispositive of damages for class proceedings in setting quantum, when not dependent on financial losses.

Claimant(s): McIntosh
Defendant(s): Legal Aid Ontario and Reddick

Causes of action – Tort for intrusion upon seclusion

Significant points of law – breach of privacy

Judgment – Awarded damages of CAN \$10,000.

Legal costs – CAN \$6,500.

Observations – Damages set for general damages; special damages refused as no connection between loss of employment with tortious conduct.

Claimant(s): Albayate
Defendant(s): Bank of Montreal

Industry – Finance

Causes of action – Breach of privacy.

Mitigating/aggravating factors – Not intentional, apologized and recognized issue immediately.

Significant points of law – Breach of privacy.

Judgment – Awarded damages of CAN \$2,000.

Legal costs – CAN \$0.

Observations – Damages for change of address without consent, statements sent to ex-husband's address; nominal damages awarded and claims for negligence, breach of contract dismissed.

Claimant(s): Chandra
Defendant(s): Canadian Broadcasting Corporation

Industry – Media

Causes of action – Intrusion upon seclusion.

Significant points of law – consideration of whether PIPEDA ousts common law claims.

Observations – Court considered whether breach of privacy can be claimed – PIPEDA does not oust common law claims.

Claimant(s): Jane Doe
Defendant(s): Defendant

Causes of action – Breach of confidence

Significant points of law – Consideration of whether action would lie for breach of confidence – sharing of intimate photos.

Judgment – Awarded damages of CAN \$100,000.

Observations – Decision appealed, precedent value in doubt as sent back to trial for consideration.

Claimant(s): Vanderveen
Defendant(s): Waterbridge Media

Industry – Media

Causes of action – Breach of privacy, appropriate of personality.

Significant points of law – Filming of jogger without her consent.

Judgment – Awarded damages of CAN \$4,100.

Observations – Privacy right prevails over non-public commercial interest.

Other key developments

Media interest – Media interest in the disclosures of breach incidents.

Guidance – The OPC has issued a Fact sheet on the upcoming amendments to PIPEDA and the mandatory breach notification. The OPC also provides guidance on reporting breaches to the OPC. More guidance documents should come out once the regulations are in force.



David Craig
+1 416 814 5812
david.craig@pwc.com



Jordan Prokopy
+1 647 822 6101
jordan.prokopy@pwc.com



Constantine Karbaliotis
+1 416 869 2463
constantine.n.karbaliotis@pwc.com



Maria Koslunova
+1 416 687 8791
maria.koslunova@pwc.com

China

National law

National law – Marking a milestone, the Chinese Cybersecurity Law (“CSL”) sets up a comprehensive legal framework for data protection and cyber security including how to deal with personal data breach.

Regulator – China’s CSL supervisory agencies feature a general regulation plus sector focus system, which is comprised of three major supervisory agencies, the Cyberspace Administration of China (“CAC”), the Ministry of Industry and Information Technology of China (“MIIT”) and the Ministry of Public Security (“MPS”), and multiple industry regulators, such as the Central Bank of China, the China Banking Regulatory Commission (“CBRC”), the China Insurance Regulatory Commission (“CIRC”), the China Securities Regulatory Commission (“CSRC”), the Ministry of Education, the Civil Aviation Administration of China (“CAAC”), and so forth.

The CAC leads the charge of CSL supervision and administration by taking responsibility for comprehensive arrangement and coordination of work in connection with cyber security. In particular, this lead agency oversees online content regulation and makes rules for national security review of network products and services and cross border data flow. In 2017, the CAC released the National Cyber Security Incident Emergency Plan (“NCSIEP”) outlining the general roadmap for handling data breach incidents.

The MIIT regulates the telecommunication and network industry and general personal information protection of telecommunication and internet users. As a step to implement the NCSIEP, also in 2017, this agency came up with the Public Internet Cyber Security Incident Emergency Plan (“PICSIEP”) which is aimed to outline the incident coping strategy for basic telecommunication carriers, domain name registration authorities and domain name registration service agencies.

The MPS implements the Multi-Level Protection Scheme (“MLPS”), a major IT/cyber security protection system which was adopted much earlier than the CSL and still takes center stage under the CSL. It also investigates crimes in connection with personal information and cyber security.

The industrial regulators play a primary role in protecting personal information and responding to data breach incidents in their respective sector, while maintaining close communications and collaborations with the foregoing three major supervisory bodies.

Enforcement powers – The CSL and a variety of implementing rules set forth the extensive enforcement powers of the regulators. Generally speaking, the regulators can investigate a case by the following means:

- Interview;
- Inspection;
- Appraisal;
- Evidence collection, including on-site or remote e-discovery;
- Seizure;
- On-site inspection;
- Detention (police only).

Penalties –

Law: RMB 1 million.

Imposed: In 2017, RMB 0.5 million pecuniary penalty on: Sina Weibo for not effectively preventing and stopping the spread of pornographic and ethnic hatred information on its platform;

Tencent for not effectively preventing and stopping the spread of violent, terrorism, false and pornographic information on its Wechat platform.

Breach notification – Yes

Article 22 of the CSL: ...Network products and services providers notify users and report to relevant authorities in a timely manner when they find that their network products or services have security defects, loopholes or other risks;

Article 25 of the CSL: ...in the occurrence of any incidents endangering network security, network products and services providers shall report to competent authorities.

Article 42 of the CSL: ...When personal information is or might be divulged, damaged or lost, network operators shall take remedial measures immediately, notify the users in a timely manner and report to competent authorities.

2017 notable issues

Breakdown of enforcement action

In China there is no compulsory requirement on enforcement action disclosure in the field of data protection and cyber security. The statistics below are based on publicly available information, especially those released on the official websites of the supervisory agencies. They are, however, by no means exhaustive or complete.

Type	No.
Monetary Penalty Notice (i.e. fines)	N/A
Undertakings	>164
Enforcement notices	>4900
Prosecutions	>4900

Notable enforcement action/investigations concluded

An unidentified airline

Date of enforcement: 2017

Industry – Transport and leisure

Incident – A staff of the airline, in conspiracy with others, hacked into the intranet of the company, stole passengers' personal information and sold it to scam gangs gaining illegal interest of more RMB 6 million.

Mitigating/aggravating factors – N/A

Enforcement action – This case was investigated by a city level police department.

Regulator comment – “Inside job” is a very important characteristics for data breach cases.

Observations – In China, internal control and compliance remain a weak point of company's sustainable development, and poses significant threat to personal data protection and cyber security. Oftentimes, it is until the occurrence of data breach incidents that a company has a clear mind about the importance of an effective compliance system. With the gradually increasing CSL enforcement, more Chinese companies are embracing the idea of ex ante compliance building.

Other key developments

Enforcement trends – The enforcement agencies look into extensive personal information categories, because the breached personal information is fairly diversified, ranging from ID, phone number, home address, to mobile phone address book, bank account and password, shopping records, and activity trails, etc.

- The investigations normally dig into the whole value chain of black market, covering data suppliers, intermediaries and end users.
- The enforcement agencies attach attention to both the government or company employees who have access to personal information at work, and hackers who use fishing websites, Trojan, free WIFI, and malwares to steal data.
- Thanks to China's multi-faceted implementing system, cross-agency enforcement is not rarely seen. For instance, apart from industry regulators, the policy may be involved where criminal liabilities can be expected or MLPS issues are relevant.
- The decentralized feature of the online world has made law enforcement highly rely on whistle-blow to spot leads.
- The multilateral network governance system advocated by the CSL has made online platform operators an important pillar of law enforcement. They bear the primary responsibility to implement personal data protection, data breach notification, real-name system, online content regulation, and cooperation with the authorities in daily inspection or official investigations.
- Although the enforcement force of the CAC and MIIT are chiefly sitting at provincial level, the grass root agencies of the MPS could reach almost any corner and thus play a major role in day-to-day CSL enforcement.

Sector focus – Education, real estate, express delivery, job hunting, and transport.

Litigation

Legal overview

Claims that may be brought by individuals:

In the Mainland China, claims can be brought under: the CSL, the Consumer Interest Protection Law, Torts Law, breach of confidence, defamation, misuse of private information, harassment, employment laws, etc.

Key questions

Can claimants bring class actions?

There is no class action system in the US or UK sense. The most similar system is called “representative litigation”, whereby the common claimants can nominate a representative to lead the proceeding. Having said that, if the breach of consumer data is in connection the privacy policy, a standardized document constituting the legal basis of data collection and use, and this document is profoundly unfair, public interest lawsuit can be lodged.

Have they been used for data protection claims?

Not yet, according to publicly available information.

Are “no-win-no-fee” arrangements available?

Contingency fees are allowed in China.

Have they been used for data protection claims?

N/A

Is third party litigation funding available?

Not yet

What are the barriers (or perceived barriers) to litigation?

Chinese are not readily aware of the interest in personal information protection;

- Litigation cost is high;
- Evidence collection is difficult, especially when data breach is connected with high technologies;
- Transparency of government's enforcement actions is yet to be improved, so follow-up litigations are relatively rare;
- Litigation is not a popular culture.

Notable cases

Claimant(s): Ye Zhu

Defendant(s): Baidu Wangxun Technology Ltd. Co. ("Baidu")

Industry – Online technology and telecoms

Causes of action – In 2013, Ye Zhu sued Baidu for infringing upon her privacy by using cookies to track her online behaviors and popping up unwanted advertisements customized on the basis of the information exchanged through cookie.

Mitigating/aggravating factors

- Baidu collected and used information which could not identify an individual;
- Baidu did not make public the cookie information and Ye Zhu's search key words;
- Baidu provided privacy policy which informed users of how to modify or unset cookies;
- The privacy policy was put at a place which was consistent with industry practice.

Significant points of law

- Torts Law: network service providers/users shall be held accountable where it infringes upon others civil rights through internet;
- Provisions of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests: Where a network user or network service provider causes harm to a natural person by using the Internet to make public the natural person's genetic information, medical records, health examination data, criminal records, home address, personal activities or other personal privacy and personal information, the competent people's court shall uphold the claims made by the infringed party and the network user or network service provider shall be held accountable.

Judgment – Ye Zhu's claims were dismissed, but the judgment of the first instance court was overturned upon appeal.

Damages – N/A

Legal costs – The total RMB 800 litigation fees (RMB 400 for first instance and the same amount for appeal) were borne by Ye Zhu. The judgement did not address who should pay the legal counsel's fee, if any.

Observations

- It's largely a common understanding that the authority needs to strike a balance between personal information/privacy protection and freedom;
- The newly released recommended national standards for personal information security specification addresses cookie issues in a privacy policy template attached to the document. Nonetheless, without a specific regulation or official interpretation, cookie remains the focal point of debate in the context of data protection, and more controversial cases can be expected.

Other key developments

Media interest – The media are interested in reporting enforcement actions, new rules, and government officials' remarks addressing enforcement trends and patterns.

Guidance – In 2017, the CAC released NCSIEP outlining the general roadmap for handling data breach incidents.

The MIIT regulates the telecommunication and network industry and general personal information protection of telecommunication and internet users. As a further step to implement the NCSIEP, also in 2017, this agency came up with the PICSIEP which is aimed to outline the incident coping strategy for basic telecommunication carriers, domain name registration authorities and domain name registration service agencies.



Jing Wang
+86 (10) 8540 4630
jing.wang@ruibailaw.com



Annie Xue
+86 (10) 8540 4602
annie.xue@ruibailaw.com

Georgia

National law

National law – Law on Personal Data Protection and Law on Enforcement Proceedings.

Regulator – Personal Data Protection Inspector.

Subject to respective violation, the Personal Data Protection Inspector either issues warning or imposes the penalty to the violator. If the penalty is not paid within 1 month, the Personal Data Protection Inspector sends the case to the National Bureau of Enforcement for mandatory enforcement procedures.

Enforcement powers – The Inspector has the authority to carry out respective inspections, give recommendations, issue warnings or impose administrative penalties, draw up an administrative offence report and review relevant cases.

Penalties –

Law: The penalty depends on the type of violation. Ordinary penalties vary from 100 to 3000 GEL and for other breaches within 1 year – from 500 to 10 000 GEL.

Imposed: GEL 10,000.

Breach notification – No.

2017 notable issues

Breakdown of enforcement action

Type	No.
Monetary Penalty Notice (i.e. fines)	145
Undertakings	270
Enforcement notices	53
Prosecutions*	11

* Cases were sent to the Office of the Prosecution for the possible elements of crime

Litigation

Legal overview

Claims that may be brought by individuals – For any violation of the law on Personal Data Protection, application can be made to Personal Data Protection Inspector or to the court.

There are not many court cases, since applications are usually made to the Personal Data Protection Inspector.

Key questions

Can damages be obtained for non-financial loss?

Yes, an action may be brought for moral damages too.

Have they been used for data protection claims?

Not yet, according to publicly available information.

Can claimants bring class actions?

Yes

Are “no-win-no-fee” arrangements available?

No

Is third party litigation funding available?

No



Vano Gogelia
+995 551 02 94 94
vano.gogelia@pwc.com



Nino Usharauli
+995 599 808072
nino.usharauli@ge.pwc.com

India

National law

National law – In India there is no comprehensive data protection regulation. Privacy-related provisions were defined in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Additional sector-specific privacy provisions defined in various other Acts including the Aadhaar Act and Unified License Agreement (for telecom). Aadhaar is a 12-digit unique identity number that can be obtained by residents of India, based on their biometric and demographic data.

Regulator – The Unique Identification Authority of India (“UIDAI”) collects the demographics (name, gender, address, date of birth, mobile number, email address) and biometric (photo, fingerprints, iris scan) information of Indian residents. UIDAI has formulated, and governs, the laws and regulations that are specific to Aadhaar.

Enforcement powers – UIDAI is responsible for end-to-end management of Aadhaar including operations as well as security and privacy. Its enforcement powers include issuing directives to the various environment partners and taking action against them in case of any non-compliance. Some of the regular actions are:

- Cancellation/suspension of licenses;
- Imposing fines on environment partners; and
- Criminal action against environment partners.

Penalties –

Law:

Offence	Penalty
<ul style="list-style-type: none"> • Impersonation at time of enrolment by changing demographic or biometric information 	Imprisonment for up to three years; and/or Fine up to 10,000 rupees.
<ul style="list-style-type: none"> • Tampering with data in the Central Identities Data Repository (“CIDR”) 	
<ul style="list-style-type: none"> • Other impersonation 	Imprisonment for up to three years; and/or
<ul style="list-style-type: none"> • Disclosing identity information 	Fine up to 10,000 (individual)/or 100,000 rupees (company).
<ul style="list-style-type: none"> • Unauthorised use by requesting entity 	
<ul style="list-style-type: none"> • Unauthorised access to CIDR 	Imprisonment for up to three years; and/or Fine up to 1m rupees.
<ul style="list-style-type: none"> • Non-compliance with intimation (notification) requirements 	Imprisonment for up to one year; and/or Fine up to 10,000 (individual)/or 100,000 rupees (company).
<ul style="list-style-type: none"> • General penalty 	Imprisonment for up to one year; and/or Fine up to 25,000 (individual)/or 100,000 rupees (company).

Imposed: According to media reports in December 2017, UIDAI imposed an ‘interim penalty’ of 25m rupees (\$383,000 USD) on Bharti Airtel (a requesting entity under the Aadhaar Act), the largest telecom service provider of India.

Breach notification – UIDAI has mandated environment partners to “report promptly to the Authority any security incidents affecting the confidentiality, integrity and availability of information related to the Authority’s functions” (Reg. 5, Aadhaar (Data Security) Regulation, 2016)

Sector-specific regulation

IT and cyber security

Law – Information Technology Act, 2000 (“IT Act”)

Regulator – Ministry of Electronics and Information Technology (“MeitY”). Governance for this area is done through multiple bodies, the main agency being Computer Emergency Response Team, India (“CERT-In”).

Enforcement powers – Roles, responsibilities and powers of the various bodies are defined in the IT Act. These include:

- Investigating an incident;
- Power to enter any public space and search and arrest without warrant any person found therein who is reasonably suspected of having committed (or of committing or of being about to commit) any IT Act offence;
- Deciding on the quantum of punishment and any fine to be imposed; and
- Adjudicating matters (where the claim does not exceed 50m rupees).

Penalties – Law – For failure to protect data a body corporate shall be liable to pay damages by way of compensation to the person affected.

Anyone contravening IT Act rules or regulations, where no penalty has been separately provided, shall be liable to pay compensation to the person affected or a penalty, each being up to 25,000 rupees.

The penalty for breach of confidentiality and privacy is imprisonment for up to two years and/or 100,000 rupees.

In cases of offending by companies, any person who was (at the relevant time) in charge of and responsible to the company for the conduct of its business, shall be guilty of the contravention.

Breach notification – reporting of cyber security incidents is mandatory for service providers, body corporates, data centers, intermediaries and others (Sec. IT Act, read with Rule 12(1) (a)).

Telecommunications

Regulator – Department of Telecommunication (“DoT”).

Penalties – law – for a security breach caused by inadequate protections on the part of a licensee, the penalty is up to 500M rupees.

Criminal proceedings can also be initiated, for example under the Indian Telegraph Act, IT Act, Indian Penal Code (“IPC”) or Criminal Procedure Code (“Cr PC”).

Breach notification – telecoms companies must create facilities for the monitoring of intrusions, attacks and frauds on their facilities and provide reports on the same to the DoT (cl. 39.10(i), Unified License Agreement).

Banking

Law – banks must have a board-approved cyber security policy which is distinct from their IT Policy/IS policy.

Regulator – Reserve Bank of India (“RBI”).

Enforcement powers – RBI is fully owned by the Government of India and manages the financial institutions and their functioning, including:

- Maintaining public confidence in the system;
- Protecting depositors’ interests;
- Providing cost-effective banking services to the public; – Prescribing broad parameters of banking operations within which the country’s banking and financial system functions; and
- Supervision of financial institutions.

Penalties imposed – according to media reports 60M rupees was paid by Yes Bank in October 2017 for breaching RBI rules on classifying non-performing assets and failing to report a security incident involving its ATMs in timely manner.

Breach notification – security incidents must be informed to RBI within two to six hours of detection.

Critical Information Infrastructure

Regulator – the National Critical Information Infrastructure Protection Centre (“NCIIPC”) is an Indian government organisation created in January 2014 under the IT Act (through a gazette notification). Based in New Delhi, India, it is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.

Organisations which have been notified under the critical information infrastructure regime (“CIIs”) need to comply with the NCIIPC Control guidelines and evaluation framework.

Enforcement powers – NCIIPC engages with the various CIIs on a regular basis and communicates as per defined protocols.

Penalties – law – no penalties have so far been defined by the NCIIPC.

Breach notification – NCIIPC has asked the CIIs to define a mechanism for reporting data breaches, and has prepared a standard form for reporting incidents.

2017 notable issues

Notable enforcement action/investigations concluded:

Bharti Airtel and Airtel Payments Bank

Date of enforcement: December 2017

Industry – Online technology and telecoms

Incident – LPG (cooking gas) subsidy payments worth 1.9bn rupees were allegedly routed to over 3 million Airtel payment bank accounts, with some of the accounts apparently having been opened without informed user consent. This was in violation of the Aadhaar Act and its Regulations.

Mitigating/aggravating factors – Airtel has two distinct licenses for carrying out Aadhaar electronic KYC (“eKYC”) transactions. One is for the telephone company (to register customers for a SIM card) and the other for its payment bank (to open new accounts). It is believed that a large number of Airtel payment bank accounts were opened without user consent when they came for linking their SIM card with the Aadhaar.

Enforcement action – UIDAI temporarily barred Bharti Airtel and Airtel Payments Bank from conducting Aadhaar-based SIM verification of mobile customers using eKYC process as well as eKYC of payments bank clients.

UIDAI also asked PwC to conduct an audit of Airtel and Airtel Payments Bank to ensure they are in compliance with Aadhaar Act.

The DoT and RBI conducted an assessment to ensure compliance with their respective prescribed policies and procedures.

According to media reports, Airtel submitted to UIDAI an interim penalty of 25m rupees (\$383,000 USD).

All the money which was credited to the Airtel Payments Bank had to be refunded to the users’ choice of bank account.

Observations – With the introduction of Aadhaar and its widespread usage, people are now becoming more aware about their privacy. With this enforcement action the importance of user consent came to the fore. Since the Aadhaar Act is comparatively new, compliance is still in nascent stage. The environment is slowly learning about it and taking steps to remain compliant.

Axis Bank, eMudhra and Suvidha Infoserve

Date of enforcement: February & March 2017

Industry – Finance, insurance and credit (Axis Bank); online technology and telecoms (eMudhra & Suvidha)

Incident – Action by UIDAI for storing individuals' biometric data without consent and performing multiple authentication transactions. UIDAI lodged a complaint with Delhi police against the three companies for violating the Aadhaar Act and Regulations. It was done after UIDAI found the same biometric match in multiple consecutive transactions which could be only done if the biometric data was stored.

Mitigating/aggravating factors – It was found that biometrics were being stored in the local application developed by Suvidha Infoserve. The stored biometrics were used to perform transactions after authenticating from the UIDAI database. Out of the transactions, 194 were performed through Axis Bank, while 91 and 112 were performed through Suvidha Infoserve and eMudhra respectively. The UIDAI flagged the transactions after noticing that many of them were performed concurrently, indicating a common element behind the operations. The simultaneous multiple successful transactions and exact biometric match score in several successive transactions is not possible without use of stored biometrics.

Enforcement action – The authentication transaction facility for the three entities was temporarily suspended pending further investigation.

The UIDAI filed a police complaint against the three entities for attempted unauthorised authentication and impersonation by illegally storing Aadhaar biometric data.

A fine of an undisclosed amount was also imposed on the three entities.

Observations – This was a significant development in the Aadhaar environment. After the incident a number of new directives, notices and guidelines were issued by the Authority to build in better security and privacy measures.

Yes Bank

Date of enforcement: October 2017

Industry – Finance, insurance and credit

Incident – Yes Bank failed to report to RBI in a timely manner a security incident relating to its ATMs. Card data of 3.2 million users was stolen between 25 May and 10 July 2016 from a network of Yes Bank ATMs managed by Hitachi Payment Services Pvt. Ltd.

Mitigating/aggravating factors – It was only in September that year that banks and payments services providers became aware of the extent of the breach.

Enforcement action – RBI fined Yes Bank of 60m rupees (approximately \$1 million USD).

Regulator comment – No official comment was given by RBI, however they released a press notification which said that they had imposed the monetary penalty “for non-compliance with the directions issued by RBI on Income Recognition Asset Classification norms and delayed reporting of information security incident involving ATMs of the bank.”

Observations – RBI has mandated a number of requirements as part of its directives and performs regular assessment of the same to check for compliance. RBI has taken such measures in the past as well which has made sure that the Banks take compliance seriously.

Other key developments

Enforcement trends – usage of Aadhaar has recently increased greatly and UIDAI have been proactive in identifying compliance issues and taking steps to address them.

Sector focus – since there is no overarching body for privacy, sector-specific regulators are focused on their respective areas. CERT-In looks after the entire spectrum with focus on financial services and government, as well as other critical infrastructure.

Litigation

Legal overview

Claims that may be brought by individuals – the IT Act provides for remedies where contravention of the Act has caused injury or damage. Claims can be up to 50m rupees (\$750,000 USD).

In addition personal privacy violations are prohibited (s. 66E): “whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person.” The penalty is up to three years imprisonment and/or a fine up to 200,000 rupees.

Publicly-available precedents on the application of these laws are limited.

Key questions

Can damages be obtained for non-financial loss?

Yes, they can also be claimed for injury.

What are the barriers (or perceived barriers) to litigation?

Limited knowledge on the part of individuals of the IT Act and privacy law generally.

Notable cases

Generally no details on specific cases are available in the public domain, however recently the widespread usage of Aadhaar has sparked privacy fears among the population, privacy group and civil rights activists leading to a case against Aadhaar regime.

This is not related to any specific incident, but rather the case concerns the overall validity of the Aadhaar and its linkage with banking, telecoms and other databases.

Claimant(s): Privacy groups, civil rights activists and certain individuals

Defendant(s): Government of India

Industry – Other: national government

Causes of action – widespread usage of Aadhaar sparking privacy fears which have been continuously denied by UIDAI and the Government of India.

Mitigating/aggravating factors – Recently the Indian government has made Aadhaar mandatory for a number services and benefits, and many private sector organisations have started to require Aadhaar for them to provide their services.

This has sparked privacy fears and there have been worries about Aadhaar becoming a tool for mass surveillance. UIDAI has denied this and reiterated that Aadhaar implements security and privacy by design and does not allow any possibility of profiling.

Significant points of law – the matter is currently being heard in India's highest court.

Observations – this is a key case in the history of India's technological landscape. Since Aadhaar forms the backbone of many of the country's digital initiatives, the outcome of this judgment will affect the entire security and privacy landscape and has the potential to materially affect the country's social and economic development.

Other key developments

Legislative and regulatory changes – In August 2017 the Indian Supreme Court gave a landmark verdict on privacy. A nine-judge bench ruled that Indians enjoy a fundamental right to privacy, under Article 21 of the Indian constitution.

Many cases are now being seen in light of this ruling, including the case on legal validity of Aadhaar being one of them. Aadhaar is being used as a fundamental requirement to push the Digital India initiative and hence that has serious implications.

- The Government of India constituted a Committee of Experts under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna to study various issues relating to data protection in India and make specific suggestions on principles to be considered in a draft Data Protection Bill. The objective is to “ensure growth of the digital economy while keeping personal data of citizens secure and protected.”
- A White Paper has been drafted to solicit public comments on what shape a data protection law must take. On the basis of the responses received, the Committee conducted public consultations with citizens and stakeholders. The seven key principles mentioned on which privacy framework could be based upon in the country include:
- Technology agnostic law;
- Be applicable to the private sector and the government, maybe with different obligations though;
- Informed and meaningful consent;
- Minimal and necessary data processing;
- Data controller must be accountable for any processing;
- Establishing a high-powered statutory authority for enforcement, supported by a decentralised enforcement mechanism; and
- Penalties for wrongful data processing to ensure deterrence.

It is expected that a detailed Bill will be prepared and shared with the Parliament, becoming an Act over the course of 2018.

Where currently the Indian privacy provisions mentioned in parts in various Acts or individual sector specific provisions, with the Data Protection Bill, India's privacy framework could see a comprehensive shift.

Other key developments

Media interest – in India there has been a major push for digitisation and accordingly there has been a lot of focus on ensuring security. Any breach of security or privacy, however small or large, is promptly reported in the media and followed up diligently.

With increasingly wide application of Aadhaar, there is a huge interest in the media regarding the national privacy debate. All the top media houses (both print and electronic) are covering the Aadhaar litigation and its implication for data protection.

Guidance – some of the Authorities which have put in robust frameworks are listed above, including MeitY, UIDAI, RBI, NCIIPC and DoT. As and when required, the above mentioned regulators release additional guidelines/notification for their environment partners to comply with.

Privacy groups/lobbies – A number of privacy groups are currently working on various privacy-related issues.

- Activists are participating in the drafting of the Data Protection Bill by providing relevant comments and discussing with the members of the Committee drafting the bill.
- Another group of privacy activists is actively fighting against Aadhaar and its mandated use for various services.



Rajinder Singh
+91 9873264886
rajinder.singh@pwc.com



Faiz Haque
+91 8130064263
faiz.haque@pwc.com

Japan

National law

National law –

- Act on the Protection of Personal Information (Act No. 57 of 2003) (the “APPI”). Amendments to APPI came into effect on 30 May 2017.
The amendments to APPI has introduced a restriction on the transfer of personal data to foreign countries, which is similar to the restrictions under GDPR. The concept of anonymously processed information has also been introduced into APPI. A company who produces anonymously processed information is required to comply with the restriction stipulated by APPI in the course of producing and keeping such information.
- The Act on Specified Commercial Transactions (Act No. 57 of 4 June 1976) and the Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 17 April 2002) provide restrictions on direct marketing (the “Direct Marketing Acts”).
- The Basic Act on Cybersecurity (Act No. 104 of 2014) provides the basic principles of cybersecurity.

Regulator –

- Under the current APPI, the regulator is the Personal Information Protection Commission (“PPC”).
- The regulators are the Financial Services Agency/Consumer Affairs Agency/Ministry of Internal Affairs and Communications.
- The regulator is the Ministry of Internal Affairs and Communications.

Enforcement powers – (1) PPC has the power to request further information and recommend that a personal information handling business operator (**Business Operator**) who violates APPI should cease the violation. If they do not take the recommended measures, PPC may order them to take the recommended measures.

A failure by a Business Operator, who violates APPI, to comply with PPC’s enforcement order would constitute a criminal offence which includes imprisonment (in the case of natural person) and financial penalties.

(2) Issuing administrative orders including, but not limited to, to suspending or prohibiting business by those who violate these acts.

A breach of duties under these acts would constitute a criminal offence imprisonment (in the case of natural person) and financial penalties.

Penalties –

Law:

- Up to JPY 500,000.
- The Act on Specified Commercial Transactions can impose penalties up to JPY 3,000,000. The Act on Regulation of Transmission of Specified Electronic Mail can impose penalties up to JPY 1,000,000.

Imposed: No criminal offence including financial penalties has been reported yet to date.

Breach notification – There is no notice of breach obligation under the APPI. However, PPC requires the Business Operator to exercise efforts to report any data breach to PPC.

Sector-specific regulation – There are no sector-specific regulations other than APPI. However, PPC and other regulators have jointly issued the guidance applicable to medical sector and the guidelines applicable to the following sectors:

- Financial sector;
- Telecommunication sector;
- Broadcasting sector;
- Post service sector;
- Correspondence delivery business sector; and
- Genetic information business sector.

These guidelines provide more detailed duties and procedures, applicable for each sector, within the framework of APPI.

Depending the sector, the following regulators may be relevant: PPC and the Financial Services Agency, Ministry of Internal Affairs and Communications, Ministry of Economy and Trade and Industry, and Ministry of Health, Labor and Welfare.

2017 notable issues

Breakdown of enforcement action

The PPC was established in 2016. Before the PPC was established, incidents of disclosure of personal information were dealt with by the ministry responsible for the industry in which the leak occurred.

PPC disclosed the status of the enforcement actions by each ministry from 2005 to 2016. The numbers below are based on that disclosure.

According to the disclosed documents (i.e., from 2005 to 2016), there were no monetary penalty notices.

Type (from 2005-2016)	No.
Collection of reports	326
Recommendation	8
Advice	3

Notable enforcement action/investigations concluded

Benesse Corporation

Date of enforcement: 26 September 2014

Industry – Education and childcare

Incident – A temporary employee of a Benesse contractor had stolen the personal data of Benesse customers and sold it to a mailing list broker. The personal data of about 30 million customers was leaked.

Mitigating/aggravating factors – Overconfidence in the security system of Benesse Corporation; lack of IT literacy.

Enforcement action – The authority (Ministry of Economy, Trade and Industry) recommended that Benesse Corporation improve its internal control environment and supervision of contractors.

Observations – The employee was sentenced to two years and six months’ penal servitude.

Mitsubishi UFJ Morgan Stanley (former name: Mitsubishi UFJ securities)

Date of enforcement: 25 June 2009

Industry – Finance, insurance, and credit

Incident – An employee working as a system engineer, had stolen the personal data of Mitsubishi UFJ Morgan Stanley customers and sold it to a mailing list broker. The personal data of about 50 thousand customers was leaked.

Mitigating/aggravating factors – Lack of a management system.

Enforcement action – The authority (Finance Service Agency) recommended that Mitsubishi UFJ Morgan Stanley improve its internal control environment and supervision of employees.

Observations – The employee was sentenced to two years' penal servitude.

Other key developments

Enforcement trends – The number of enforcement actions is decreasing. For example, the number of collection reports was 87 in 2005, and 6 in 2016.

Litigation

Legal overview

Claims that may be brought by individuals – Article 709 of the Japanese Civil Code prescribes damages in torts. When a data protection breach is evaluated as illegal under Article 709, a claimant can demand damages.

Japanese Civil Code has not been amended for enforcing a data protection breach.

Key questions –

Can damages be obtained for non-financial loss?

Yes. In Japan, a person can claim compensation by damages in torts.

Can claimants bring class actions?

No, they cannot.

Are “no-win-no-fee” arrangements available?

A lawyer determines his or her own fee at will, so a lawyer may take on a data protection breach matter on a “no-win-no-fee” basis.

Is third party litigation funding available?

No, it is not.

What are the barriers (or perceived barriers) to litigation?

Amounts awarded for damages are small in Japan. On the other hand, lawyers' fees are generally expensive. Therefore, it is common that filing a suit is not worth the expense involved.

Notable cases

Claimant(s): Victims of leaking of private information (14 people)

Defendant(s): TBC Group CO,LTD

Industry – Health (Aesthetic)

Causes of action – Civil Code.

Significant points of law – This case involved a complaint that the claimants' private information could be accessed on the defendant's web site by anyone. Defendant subcontracted the third party creating and maintaining the web site. But, the court granted claimants' claim for the reason that defendant directed and supervised the third party.

Judgment – See above.

Damages – JPY 22,000 to 35,000 per person.

Observations – Damages in this case (up to JPY 35,000) are some of the highest damages per person in Japanese litigation from what I can gather.

Claimant(s): Victims of leaking of private information (10,801 people)

Defendant(s): Benesse Corporation

Industry – Education and childcare

Causes of action – Civil Code

Damages – Claimants' claim totaled JPY590,095,000.

Observations – The day of filing of the suit is 19 January 2015, but the first trial is still proceeding.



Satoshi Mogi

+81 (0)3 5251 2725

satoshi.mogi@pwc.com

Mauritius

National law

National law – Data Protection Act 2017 will strengthen the control and personal autonomy of data subjects over their personal data, thereby contributing to respect for their human rights and fundamental freedoms, in particular their right to privacy, in line with current relevant international standards, in particular the General Data Protection Regulations (“GDPR”) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Regulator – Data Protection Office (“DPO”). The DPO is under the aegis of the Ministry of Technology, Communication and Innovation. It has been in operation since February 2009.

The head of the office is the Data Protection Commissioner. The Commissioner enjoys a wide range of enforcement powers to assist him in ensuring that the principles of data protection are observed.

Enforcement powers

- To do all such acts in connection with the carrying out of its functions;
- To obtain information as is necessary or expedient for the discharge of its functions and to exercise its powers;
- To investigate complaints reported to it;
- To delegate any of its investigating an enforcement power conferred to it by the Data Protection Act 2017;
- To carry out periodical audits of the systems of data controllers and data processors to ensure compliance with data protection principles;
- To serve enforcement notices against contraveners of the Data Protection Act 2017;
- To apply to a Judge in Chambers for a Preservation Order for the expeditious preservation of data, including traffic data, where it believes that the data are vulnerable to loss or modification;
- To seek assistance from such person or authority to assist the Commissioner in the discharge of his functions; and
- To enter and search any premise for the purpose of discharging its functions under the Data Protection Act 2017.

Penalties – law – Rs. 200,000.

Breach notification – Yes.

2017 notable issues

Litigation

Legal overview

Claims that may be brought by individuals –

Breaches of the following:

- Data Protection Act 2017;
- Section 26 of the Bank of Mauritius Act;
- Section 64 of the Banking Act;
- Section 83 of the Financial Services Act;
- Section 30 of the Financial Intelligence and Anti-Money Laundering Act; and
- Section 81 of the Prevention of Corruption Act.

Key questions

Can damages be obtained for non-financial loss?	Yes
Can claimants bring class actions?	
There is no Public Interest Litigation in Mauritius. However, if a group of people feel prejudiced against, they can bring collective actions through an association.	
Are “no-win-no-fee” arrangements available?	No
Is third party litigation funding available?	No

Other key developments

Sector-specific campaigns – People who are responsible for data protection matters in organisations (Directors, Legal Advisors, Data Protection Officer, Compliance Officer) were targeted. All sectors/industries were targeted.

Description of action taken – Workshops are usually organised by the Data Protection Office at least on an annual basis to discuss Data Protection.

A workshop was recently conducted to present the enhancements brought in by the Data Protection Act 2017 to educate stakeholders on the new legislation in order to protect the right to privacy of individuals.



Jean-Pierre Young
(+230) 404 5028
jean-pierre.young@pwc.com



Vikas Sharma
(+230) 404 5015
v.sharma@pwc.com



Doorvashi Seedoyal
(+230) 404 5067
doorvashi.seedoyal@pwc.com

Mexico

National law

National law – The Mexican Constitution recognises the protection of personal data as a fundamental right. Every individual has the right to enjoy protection of his personal data, and to access, correct and cancel such data. All people have the right to oppose the disclosure of his data, according to the law. The General Law on Data Protection Held by Obligated Parties entered into force on 27 January 2017 and aligned the laws applicable to public organisations with the laws applicable to private organisations under the Federal Law of Personal Data held by Private Parties.

Regulator – The National Institute of Transparency, Access to Public Information and Data Protection (“INAI”) is the nationwide regulator. The INAI works in coordination with 32 institutes throughout the states, which conform to the National System for Transparency, Access to Public Information and Data Protection (“SNT”).

Enforcement powers – Monitor and verify compliance with the provisions of the Federal Data Protection Law (“LFPDPPP”). INAI carries out investigations on request from data subjects or on becoming aware of an infringement;

- Make determinations in respect of the above investigations, which may include actions to be taken and/or penalties; and
- Apply to court for criminal judgement.

Penalties –

Law – The INAI has the power to issue fines per breach from 100 to 320,000 days of the General Current Minimum Wage in Mexico, which currently amounts to MXP\$88.36 or UMAs (which is a Measure and Adjust Unit). Where a breach includes processing sensitive personal data, the sanctions may be doubled.

Imposed – Approximately MXP\$32 million pesos (this is the largest penalty imposed by the INAI).

Breach notification – Yes, established in the Data Protection Regulation.

Sector-specific regulation

There are sector-specific regulations that regulate data breaches. These are enforced by, among others, the Ministry of Health, PROFECO (consumer protection regulator) and CONDUSEF (finance regulator).

2017 notable issues

Breakdown of enforcement action

There are three types of INAI procedure: rights protection, verification and penalty application:

- Rights protection: Initiated by the data subject;
- Verification: Initiated by INAI or by petition of an interested party, to verify compliance with data protection law and regulations; and
- Penalty application: As a result of Rights Protection Procedure or Verification Procedure, the INAI determines the appropriate penalty.

Rights protection procedures in 2017 –

Procedures in place (duly substantiated): 81 (28% less than in 2016)

Procedures discarded: 93 (29% less than in 2016).

ARCO rights	Occurrence	%
Access	492	46
Rectification	39	4
Cancellation	376	4
Objection	174	16

Verification procedures in 2017 –

Procedures in place: 50

Procedures completed: 39

In total, 4% less than in 2016.

Penalty application procedures in 2017 –

Procedures in place: 65 (22% less than in 2016)

Procedures completed: 75 (36% more than in 2016).

Total fines: MXP\$84,450,878,87 (Mexican Pesos, approximate 16% less than in 2016).

Principles	Occurrence	%
Legality	124	33.24
Accountability	99	26.54
Notice	68	18.23
Consent	33	8.85
Fidelity	32	8.58
Quality	9	2.41
Proportionality	5	1.34
Purpose	3	0.80

Most affected sectors by INAI's penalties:

Industry	Fines (Mexican Pesos)
Financial and insurance	MXP\$183,705,889
Media	MXP\$46,605,371
Retail	MXP\$19,562,990

This information was published by INAI as of November 30th, 2017.

Notable enforcement action/investigations concluded

The regulator did not mention any specific company, the INAI granted a general statement* about the most affected sectors for infringement penalties since the data protection law was enforced in Mexico.

*Published in June 2017

Industry – Finance, insurance and credit, media, retail and manufacturing

Incident – In 2017, the INAI released details of the most affected sectors since the Data Protection Law was first enforced in 2011. These are:

- Finance and insurance, with 54 penalty application procedures;
- Media, with 28 procedures;
- Retail and manufacture, with 13 procedures.

Regulator comment – The total amount of fines imposed by the INAI between 2011 and June 2017 is MXP\$317,946,732.

Observations – INAI is a very active regulator, and regularly conducts verification procedures to ensure the legitimate processing of personal data.

Other key developments

Enforcement trends – Normalización y Certificación (“NYCE”) certifies organisations’ compliance with Data Protection Law in Mexico. At the moment there are 34 private organisations which have implemented self-regulatory schemes. INAI promotes this practice through the Innovation and Best Practices in Data Protection award.

Sector focus – The INAI is focusing on:

- Finance, insurance and credit;
- Media; and,
- Retail and manufacture.

The INAI is also very active regarding public sector data processing activities

Litigation

Legal overview

Claims that may be brought by individuals – In Mexico there is data protection legal framework for both, public and private sector as follows:

Private – The Federal Law on Protection of Personal Data held by Private Parties (also referred in this article as Data Protection Law) and its Regulation.

- Guidelines for Data Protection notice.
- Self-regulation standards, among others.

Public

- General Law of Personal Data Protection held by Regulated Parties;
- General guidelines of Personal Data Protection for Public Sector; and
- Federal Law of Transparency and Access to Public Information; among others.

The regulator is the same, the only difference is the application to public and private sectors, respectively.

Key questions

Can damages be obtained for non-financial loss?

In Mexico, damages are claimed before Civil Courts. Proceedings can be filed after a successful claim of data protection and privacy before Administrative Law Courts.

Can claimants bring class actions? Yes

If so, have they been used for data protection claims? Yes

Are “no-win-no-fee” arrangements available? Yes

If so, have they been used for data protection claims? Yes

Is third party litigation funding available? Yes

If so, have they been used for data protection claims? Yes

What are the barriers (or perceived barriers) to litigation?

Lack of widespread understanding of Data Protection Law and the inexperience of Mexican Courts in applying the legislation.

Notable cases

Claimant(s) – Not available

Defendant(s) – Banco Nacional de México (Banamex)

Industry – Finance, insurance and credit

Causes of action – The Federal Law on Protection of Personal Data held by Private Parties) and its Regulation.

Mitigating/aggravating factors – The breach corresponds to wrongful handling of Access, Rectification, Cancellation and Opposition rights (“ARCO”).

Significant points of law – Infringements to ARCO rights due to negligence in the procedure and responses provided.

Observations – Similar infringement to the largest penalty imposed in 2013, approx. MXP\$32 million pesos.

Other key developments

Sector-specific campaigns – INAI announced in February 2018 that all candidates for president, political parties and activists which process personal data to promote themselves (by text messages, mail or any other means) without Mexican citizens' consent, will be prosecuted and sanctioned.

Legislative and regulatory changes – Articles 9 and 31 of the Internal Security Law ('LSI') are said by the INAI to breach the constitutional guarantee of data protection. The INAI have challenged this law before the Mexican Supreme Court of Justice.

Media interest – In fines and infringements from both private and public sectors.

Guidance – Data Protection legal framework (including guidelines, and tools) could be fully consulted at INAI's website: <http://inicio.ifai.org.mx/>

Privacy groups/lobbies – Yes, mostly from business and finance chambers.



Wendolin Sanchez
+52 (55) 5263 8578
wendoin.sanchez@pwc.com

New Zealand

National law

National law – The Privacy Act 1993 governs data protection matters in New Zealand. New Zealand benefits from an adequacy decision of the European Commission and is likely to try to maintain this position post-GDPR by incorporating key principles of the GDPR.

Regulator – Privacy Commissioner of New Zealand (“OPC”).

Enforcement powers – Principles based legislation, allows investigation of complaints made to it and referral to the Human Rights Review Tribunal (“HRRT”) of cases that are investigated, cannot be resolved, and in the opinion of the OPC indicate further action is necessary.

The OPC has no immediate enforcement powers under the current Privacy Act 1993, all cases requiring enforcement are referred to the HRRT. The Privacy Commissioner provides an opinion, it is not a ruling and it is not legally binding.

Complaints can be made to the OPC by anyone who believes they have been subjected to an “interference with privacy” and they have broad powers to enquire into any matter if they believe the privacy of an individual is being infringed. If they find cause they can mediate or refer to the case to the Director of Human Rights Proceedings and HRRT who can take legal action. Most cases are settled during the OPC investigation process before getting to this stage.

HRRT rulings are enforceable judgements.

Penalties –

Law – None. Penalties are not specified in privacy legislation in New Zealand.

It is noted that the ceiling within the HRRT jurisdiction may be limited to NZD\$200,000 depending on the case.

Imposed – highest penalty of NZD 168,070.88 (occurred once in the last 6 years), more commonly the largest penalty is NZD 20,000 and the second largest penalty sits at this level.

Breach notification – None.

Sector-specific regulation

There are six sector specific codes that sit underneath the Privacy Act which are classified as regulations under New Zealand law. Most notably the Health Information Privacy Code. These serve to clarify matters of practice within the Privacy Act or to modify one of the principles to take into account specific circumstances. The other codes are Civil Defense, Credit Reporting, Justice Unique Identifier, Superannuation Unique Identifier and Telecommunications Industry. The rules established by a code may be more or less stringent than the underlying principles in the Privacy Act.

Regulator – The OPC is ordinarily the regulator. If the breach is in the government sector the Government Chief Privacy Officer and Government Chief Digital Officer will become involved as part of their cross government role to improve practice in this area.

2017 key issues

Breakdown of enforcement action

Type	No.
Monetary Penalty Notice (i.e. fines)	0
Undertakings	0
Enforcement notices	0
Prosecutions	

Commentary

4 cases were referred to the Director of Human Rights Proceedings in the year to 30 June 2017.

37 cases were taken by complainants directly to the HRRT in the year to 30 June 2017.

The HRRT has to date only reported one case in which damages were awarded.

Other

Commentary

In the year to 31 October 2017 the OPC received 293 complaints. 53% of these were settled.

In the year to 31 October 2017 the OPC received 50 data breach notifications.

5 agencies were publicly named for non-compliance with the Privacy Act in the year to 30 June 2017.

There were 2 high profile investigations (Hager and Bradbury).

Notable enforcement action/investigations concluded

Accident compensation corporation

21 July 2017

Industry – Health

Incident – Information relied on in ongoing weekly compensation payments decision was not accurate or up to date.

Mitigating/aggravating factors – Prompt review and acknowledgement that the decision had been made in breach of Privacy Principle 8 (reasonable steps to ensure information was accurate, up-to-date, complete and not misleading) with payments reinstated and back-dated. Letter of apology sent, accepted as both immediate and genuine. ACC is committed to assessing and improving its privacy practices and has disclosed measures in place.

Regardless, a causal connection was established between the termination of compensation payments and feelings of humiliation, loss of dignity and injury to feelings. This emotional harm was considered more than trivial or of a passing nature.

Enforcement action – Declaration that interference with privacy occurred.

Damages awarded in the amount of NZD 7,500.

Observations – This is the only case yet reported in 2017 with any damages awarded and is therefore considered the only notable enforcement action. This is consistent with a single case in 2016, although there were 7 in 2015 and 4 in 2014.

The following are not specifically enforcement action, but are notable matters given that the New Zealand Privacy Act is principles based and does not give direct powers of enforcement to the Privacy Commissioner outside of referral to the Human Rights Review Tribunal which heard the above case.

Individual

February 2017

Industry – Education and Childcare

Incident – An individual provided a written warning related to a job's key performance indicators to a student magazine.

A breach was identified as the information was related to the operation of the student union and disclosure was not connected to that purpose.

Mitigating/aggravating factors – Releasing the letter was seen to reach the threshold for significant humiliation, loss of dignity, and injury to feelings.

An attempt was made to settle the case, but the respondent continued to insist they had not breached the Privacy Act.

Enforcement action – The case was referred to the Director of Human Rights Proceedings who took action and went on to award NZD 18,000 in compensation and ordered the respondent to undertake training on the Privacy Act.

Observations – The student magazine was not subject to enforcement action due to an exemption existing in the Privacy Act for a news medium carrying out tasks in relation to its news activities.

Child, youth and family

March 2017

Industry – Education and Childcare

Incident – A man's son was placed in social care and the social workers noted in reports to the Family Court that there were allegations of physical abuse and inappropriate sexual conduct by the man. This information was repeated despite the man never having been charged, prosecuted or jailed for sexual offending. The man contacted CYF multiple times to advise it to correct the information, but this did not occur.

Mitigating/aggravating factors – CYF acknowledged that errors had been made, apologies and files a memorandum in the Family Court that the information was incorrect.

Enforcement action – The OPC formed a view that there had been a breach of 2 principles of the Privacy Act, that this breach had affected the man's relationships with his child and wider family and that the stigma associated with sexual offending is such that having it inaccurately recorded was sufficient to cause significant humiliation, significant loss of dignity and sufficient injury to his feelings. The case was therefore referred to the Director of Human Rights Proceedings.

Observations – This case is notable given the highly sensitive nature of the personal information involved and that it remained incorrect despite requests over a number of years.

A university

December 2017

Industry – Education and Childcare

Incident – An academic who was dismissed made an access request under the Privacy Act for all of his work emails from a 12 month period. The university refused the request.

Mitigating/aggravating factors – The extent of the request totaled over 12,000 emails. The university had made an offer to release approved emails in some form other than the totality of a computer hard drive.

Regulator comment – The OPC stated that even though emails generated in a work capacity did meet the test for personal information it was reasonable for the university to refuse to provide them in the manner requested. The mixed nature meant that the personal information was not readily retrieval and the associated exemption under the Privacy Act therefore applied.

Observations – This case is a useful illustration of the reasonableness tests that apply under New Zealand Privacy Law.

Ongoing investigations

VTNZ

Industry – Transport and Leisure

Incident – Gang members were able to obtain the address of an informant from VTNZ.

Regulator comment – The Privacy Commissioner has indicated he will be asking VTNZ for further details of the incident.

NZ Police

Industry – Criminal Justice.

Incident – A blogger complained about a request from Police to their bank for information about them.

Regulator comment – The Privacy Commissioner concluded that Police had collected this information in an unlawful way by asking for such sensitive information without first putting the matter before a judicial officer.

Observations – It is unusual for the Privacy Commissioner to offer such public comment, but there has been considerable media and public discussion on this matter. The Privacy Commissioner also pointed out that this is not indicative of mass surveillance by the Police.

Other key developments

Enforcement trends – Focus of the OPC is on increasing up-take of the online training and awareness modules that they publish.

OPC has seen increased demand from government and business to use personal information and continued concern from the public to ensure this information is used appropriately and kept safe.

Research (from the Data Futures Partnership) investigated New Zealanders' attitudes to government use of data. This found that people are more comfortable when they know why data is being collected, who is going to use it (including being able to see who had looked at their data) and what it will be used for. This ties in with OPC consideration of and participation in projects relating to the positive impacts and risks of the smart use of large data sets.

A trial was conducted in 2016 in relation to transparency reporting and a follow-up to this has occurred. This particularly considered the grounds under which information might be released to other organisations within the Government sector.

A submission was made in the United States Supreme Court in the case of *US vs. Microsoft* relating to the execution of a US search warrant to access information held outside of the US. The Privacy Commissioner has submitted that the US Supreme Court should uphold the principle against extra territorial application of legislation and noted that for data held within New Zealand this would likely breach New Zealand law. The OPC expects that mutual assistance requests and related agreements would be the lawful mechanisms.

The Privacy Commissioner is monitoring the Uber data breach, which included some New Zealanders in the 50 million affected worldwide. The OPC notes that there was a one year gap between the breach and Uber formally notifying the OPC. This is seen by the OPC as a reason why breach notification needs to be made mandatory.

The Privacy Commissioner released multiple reports on collection by the Ministry of Social Development of data from NGOs it uses as providers. The reporting found that there was insufficient consideration given to unintended consequences and recommended an alternative method be used. This inquiry was carried out under powers in the Privacy Act which allows the ability to inquire into any matter where privacy may be infringed and to provide advice to a Minister. This reporting was unusual in the tone with which the Privacy Commissioner described the issues identified and the actions of the Ministry.

Sector focus – The Privacy Commissioner has historically been seen as focused on the government and health sectors, they are actively trying to change this perception to emphasize the message that everyone has a responsibility to protect privacy.

Litigation

The culture in New Zealand is not generally litigious. This is evidenced in the privacy domain by the percentage of OPC investigations that are settled rather than proceeding to any further action (53% settled of the cases raised with OPC, less than 2% referred to HRRT, remainder either found to be no breach or closed for other reasons).

Legal overview

Claims that may be brought by individuals – Claims are generally brought under the Privacy Act, although elements of the Human Rights Act are sometimes also considered.

A case can be referred by the Privacy Commissioner to the Human Rights Review Tribunal through the Director of Human Rights Proceedings or taken directly to that body by a complainant. They are then assessed and where appropriate heard as a case under the relevant act. These are not specific to a data protection breach, but provide a legislative mechanism by which such cases can occur.

The Office of the Privacy Commissioner together with the Law Commission are pursuing law change to potentially include mandatory breach notification and enforcement powers. This was included in the briefing documentation provided by the Privacy Commissioner to the new Government and highlighted as a matter of urgency.

Key questions

What is the largest award of damages to date?

NZD 168,070.88 under the Privacy Act.

Can damages be obtained for non-financial loss?

Yes, damages for loss of benefits and for emotional harm including humiliation, loss of dignity and injury to feelings are common in Privacy Act proceedings taken to the Human Rights Review Tribunal.

What are the barriers (or perceived barriers) to litigation?

The time taken for cases to be heard through the Human Rights Review Tribunal has recently been cited in the media as a concern in this space.

Other key developments

Legislative and regulatory changes – There are proposals to amend New Zealand privacy legislation. These have been in the pipeline for a number of years, but the latest report from the OPC to the new government dated 30 November 2017 reiterates that privacy law reform has become urgent. The current status indicated is that the OPC is meeting with officials to progress drafting related to the suggested changes.

Media interest – Media interest is generally not in litigation, but in breaches or perceived breaches by the government sector.

Privacy groups/lobbies – A number of groups continue to express concern about potential surveillance by the Police, GCSB and NZSIS. These groups have become higher profile in recent years in light of the Kim Dotcom case and Nicky Hager & Martin Bradbury.



Robyn Campbell
+64 4 462 7092
robyn.k.campbell@nz.pwc.com



Drew Parker
+64 4 462 7104
drew.x.parker@nz.pwc.com

Paraguay

National law

Regulator – Ministry of Justice – Judicial Court

Enforcement powers – The penalties are applicable to entities that not comply on actualization of financial information published by entities against the limitations established in the law.

The financial information should be updated within 4 days comes to their knowledge this information.

Penalties: law – Natural or legal persons who publish or distribute information about the financial position, financial solvency or compliance with commercial and financial obligations in violation of the provisions of this Act shall be punished with fines will range, according to the circumstances, between fifty and one hundred minimum daily wages for various work activities unspecified fines will double, triple, quadruple, and so on for each recurrence of the same affected.

The minimum wage is US\$ 13 per day.

Breach notification – The person who considers himself injured by the published information should request deletion or correction. If not, penalties can be applied by the judicial authority.

A specific format is not set, but the customer or end consumer must state that such information hurts you in your current financial status.

Sector-specific regulation

Sector-specific regulations regarding data breach apply to the financial information sector.

Regulator – The Ministry of Justice – Judicial court is also the regulator for this sector.

Enforcement powers – Penalties are applicable to entities that do not comply with the limitations for publishing financial information.

The financial information should be updated within 4 days from the date that they were aware of the incident.

Penalties: law – Penalties are the same as previously mentioned.

2017 notable issues

Breakdown of enforcement action

Enforcement trends – Consumer protection law.

Sector focus – There is neither a controller definition nor a function.

The Ministry of Defense of Consumers and Users (“SEDECO”) acts as the enforcement authority in the field of National Defense Law. SEDECO and other laws and regulations govern this area of law.

Publicly or privately recognized entities, whether departmental or municipal institutions, may act as the implementing authority at the local level, prior to an agreement with the Ministry of Defense of Consumers and Users (“SEDECO”).

SEDECO can be considered as a controller in relation to consumer defense only. This institution does not have faculties regarding to personal data matters.

Litigation

Legal overview

Claims that may be brought by individuals – Claims under the Data Protection Law or the Consumer Defense Law.

The person who suffers the damage as a result of the published information can demand before the Judicial Courts, the correction of the information and demand an indemnification of damages caused because of the published information.

Key questions

Can damages be obtained for non-financial loss?

Yes (i.e. reputational damages).

Are “no-win-no-fee” arrangements available?

Yes, they are.

What are the barriers (or perceived barriers) to litigation?

Ability to prove the damages.

Other key developments

Sector-specific campaigns – Update of personal data protection on financial status.

In 2017 a new law was approved by Congress which states that entities which publish or distribute data have to update the information within 24 hours of the receipt of payment notices.

The financial information of people who have given their consent can be published. If the published financial information would affect the business or trade status of an individual or entity it has to be constantly updated.

It is not specified how or when the update process must be done. However, the publication of financial information is limited to three years from the due date of the debts. After that period, the supplier must eliminate all records of the financial information.



Nadia Gorostiaga
+595 981 1866 490
nadia.gorostiaga@py.pwc.com



Jorge Gomez
+595 981 415 5702
jorge.g.gomez@py.pwc.com



Bruno Angulo
+595 981 122 2257
bruno.angulo@py.pwc.com

Peru

National law

National law – Personal data protection is regulated by Law No. 29733 and its Regulations, Supreme Decree No. 003-2013-JUS.

Data protection enforcement is carried out by the Ministry of Justice and Human Rights, which is entitled to impose administrative fines for breaches against personal data regulations.

Law No. 29733, Data Protection Law, and its Regulations – Supreme Decree No. 003-2013-JUS.

Regulator – The agency responsible for enforcing the data protection regime is the Director General of Transparency, Access to Public Information and Personal Data Protection, of the Ministry of Justice and Human Rights.

Enforcement powers – The Ministry of Justice has the authority to conduct inspections, receive complaints from the public and impose financial penalties on non-complying subjects.

The Ministry of Justice cannot award damages. The affected party should file a damages lawsuit against the non-complying subject for indemnity claims.

Penalties –

Law – The Ministry of Justice may impose a fine for up to 100 Peruvian Tax Units (“UIT”), which vary on a yearly basis.

For year 2018, 1 UIT equals S/. 4,150 PEN (US\$ 1,280 approx.). Maximum financial penalties would equal US\$128,000 approx.

However, in no case can the penalty exceed 10% of the company’s gross annual income.

Imposed – To date, the maximum penalty applied has been 42 UIT (US\$ 53,760 approx.), in November 2015.

Breach notification – Not mandatory.

2017 notable issues

Breakdown of enforcement action

Type	No.
Monetary penalty notice (i.e. fines)	40
Other	4

Type	Number of fines	Highest fine	Total value
Charitable and voluntary	-	-	-
Criminal justice	-	-	-
Education and childcare	7	S/. 32,400	S/. 115,830
Finance insurance and credit	3	S/. 8,100	S/. 19,440
General business	14	S/. 32,400	S/. 181,035
Health	2	S/. 40,500	S/. 51,030
Land or property services	-	-	-
Legal	-	-	-
Local government	-	-	-
Marketing	3	S/. 6,480	S/. 14,580
Media	-	-	-
Online technology and telecoms	2	S/. 8,100	S/. 9,720
Other	2	S/. 8,100	S/. 16,200
Political	-	-	-
Retail and manufacture	1	S/. 4,860	S/. 4,860
Transport and leisure	6	S/. 20,655	S/. 69,660
Total	40	-	S/. 482,355

Notable enforcement action/investigations concluded

Empresa prestadora de servicios de salud el nazareno srltda

Date of enforcement – 9 November, 2017

Industry – Health

Incident –

- Procedures for access management and privilege management for patients’ data were not documented, in breach of subsection 1 of the article 39 of the Regulations of the LPDP;
- Paper files containing sensitive personal data of the patients were stored in an unsecured area, in breach of the provided in article 42 of the Regulations of the LPDP; and,

- Controls for the reproduction of documents that contain sensitive personal data of their patients were not established, breaking the requirements of the Article 43 of the Regulations of the LPDP*.

Mitigating/aggravating factors – As a Company in the health sector, it has sensitive personal data.

Enforcement action – Sanctioned with a fine of ten tax units (10 UIT).

Litigation

Legal overview

Claims that may be brought by individuals – It is possible to submit a claim for one of the following causes:

Breach of confidence, misuse of information, hindering the exercise of Access, Rectification, Control and Objection rights. Can also claim for mishandling of information, breach of employment laws, defamation and damages claims.

The aforementioned causes of action apply in case where a plaintiff considers his or her data rights have been breached. Administrative claims at the Ministry of Justice can result in a fine to the company in breach, but will not include any damages compensation to the affected party.

Lawsuits claiming damages are heard by Peruvian civil courts. The court ruling can be subject to appeal and eventually to review by the Supreme Court. Damages claims are subject to economic valuation by the court, but judges have no uniform criteria regarding indemnity quantification.

Defamation claims are criminal procedures that are subject to review by a District Attorney, and ruled by a criminal judge. The court ruling can be subject to appeal and eventually to review by the Supreme Court. Criminal defamation claims are more common against the media for misleading the public or revealing confidential information.

Key questions

What is the largest award of damages to date?

Data protection legislation does not award any kind of compensation to the data subject.

In case of damages, a person should request compensation through a civil procedure. Damages claims in a civil court may considerably vary on a case-by-case basis.

The penalty for defamation is up to 4 years' imprisonment. However, effective jail time is seldom served.

Can damages be obtained for non-financial loss?

Yes. A person may be awarded compensation for damages related to his or her honor and reputation.

Can claimants bring class actions? No

Are "no-win-no-fee" arrangements available? No

Is third party litigation funding available? No

What are the barriers (or perceived barriers) to litigation?

Before going to court, one must have exhausted all available legal resources from the agency. After exhausting every legal resource, a case may be brought to the court's attention for its evaluation.

Notable cases

Claimant(s): Ministry of Justice (ex officio review)

Defendant(s): Sentinel Perú S.A.

Industry – Finance insurance and credit

Causes of action – Sentinel Peru was accused of providing free public access to credit and debt information of regional and municipal electoral candidates and linking it with their political information, breaching the correct use of information for credit risk analysis.

Mitigating/aggravating factors – Company's positive compliance with procedure requirements was considered as a mitigating factor.

Significant points of law – The main principles for data protection and treatment by companies were analyzed, considering the purpose for which the data was collected. The Ministry of Justice considered that Sentinel was really using credit and debt information from candidates as electoral information; exceeding the authorization granted as a risk management company for this type of private data.

Judgment – Sentinel was fined with 42 UIT (US\$ 53,760 approx.), by means of Resolution N° 085-2015-JUS/TGDP-DS.

Damages – Damages cannot be claimed in an administrative procedure.

Observations – This resolution has the highest known administrative fine applied by the Ministry of Justice for a data protection breach.

The Ministry of Justice considered that data processing purposes should be interpreted in a restrictive way, in accordance with the company's corporate purpose.

In this case, Sentinel was a credit risk analyst company, and the Ministry of Justice considered that linking this information with political information from candidates exceeded the company's purpose (to provide credit and financial information) to provide political information.

Other key developments

Media interest – Media interest is low.



Gino Menchola T
Partner
+51 1 211-6500
gino.menchola@pe.pwc.com



Carlos Fernandez Gates
Director
+51 975146040
carlos.fernandez@pe.pwc.com



Daniel Chahud Cosío
Senior Associate
+51 1 211-6500 Ext. 8022
daniel.chahud@pe.pwc.com

Russia

National law

Regulator – The Federal Service for Supervision of Communications, Information Technology and Mass Media (“Roskomnadzor”).

Enforcement powers – Roskomnadzor has the following powers:

- Issue requests to individuals and legal entities to provide any information it requires for the performance of its tasks;
- Compliance audits, including access to personal data processing systems in order to review and extract necessary information;
- Power to issue orders to eliminate discovered violations, inter alia, cease, block or destroy incorrect or illegally obtained personal data;
- Blocking of web-based services and applications where personal data is illegally processed;
- Filing of claims in court to protect rights of personal data subjects;
- Initiation of administrative offences’ prosecution in the sphere of personal data processing;
- Submission of information to police and public prosecution office in order to initiate administrative and criminal proceedings; and
- Imposition of penalties

Penalties – law – The maximum financial penalty is 75,000 Rubles per violation.

Breach notification – Not mandatory.

Sector-specific regulation

The following practice areas are subject to sector-specific regulations:

- Banking law;
- Telecom law;
- Medicine law;
- Audit law;
- Notary public law; and
- Advocates law.

Regulators – The following bodies are authorized to supervise sector-specific data protection matters:

- The Ministry of Finance and self-regulatory organizations of auditors (auditing);
- The Bank of Russia and Federal Service for the Oversight of Consumer Protection and Welfare (banking);
- Federal Service for Supervision in Health Care (medicine);

- Notary chambers (notarial services); and
- Councils of the respective advocacy chambers (advocate services).

Enforcement powers – The above named bodies have the following powers:

- Compliance audits;
- Initiation of administrative offences’ prosecution;
- Submission of information to police and public prosecution office in order to initiate administrative and criminal proceedings; and
- Internal prosecution and imposing disciplinary liability, including disqualification (for auditing companies, auditors, notaries and advocates).

The maximum financial penalty is 1,500,000 Rubles for an individual in case of banking data breach.

2017 notable issues

Breakdown of enforcement action

The numbers herein represent statistics only for the period of January-September 2017, no further official statistics are currently available:

Type	No.
Monetary penalty notice (i.e. fines)	2,588,000
	Russian Rubles
Enforcement notices	510
Prosecutions	5101

Notable enforcement action/investigations concluded

National Bureau of Credit Histories JSC

Date of enforcement – 26 August 2016 (legitimated by the court decision of 5 May 2017)

Industry – Finance insurance and credit

Incident – The regulator issued an order for the company to get consent of data subjects for using personal data collected from social networks for the purposes of conducting personal data analysis (including customer checks) for banks and other banking and finance organizations.

Enforcement action – The regulator stands on the position that personal data contained in open resources (social networks, such as VK.com, OK.ru, my.mail.ru, Instagram, Twitter) shall not be deemed publicly available data under the Russian personal data law. The company has to get specific consent to process such personal data. Courts of three instances approved the position of the regulator and denied challenge of the order.

Regulator comment – No public comments were made.

Ongoing investigations

Facebook Inc.

Industry – Online technology and telecom

Incident – The regulator announced its intention to audit Facebook's compliance with the Russian personal data law, including the requirement to localize Russian citizens' personal data within the territory of the Russian Federation in the second half of 2018.

Regulator comment – The regulator publicly announced its request to Facebook for localization of Russian citizens' personal data within the territory of the Russian Federation in 2018. If failure to comply with the localization requirement is revealed during the announced audit, an access to Facebook can be blocked in Russia despite a significant number of Russian users.

Observations – According to the regulator, information sharing was agreed at the meeting with Facebook officials held in February 2018 as a preliminary action to the forthcoming audit.

Twitter Inc.

Industry – Online technology and telecom

Incident – The regulator announced its intention to audit Twitter's compliance with the Russian personal data law, including the requirement to localize Russian citizens' personal data within the territory of the Russian Federation in the second half of 2018.

Regulator comment – The regulator publicly announced its request to Twitter for localization of Russian citizens' personal data within the territory of the Russian Federation in 2018. If failure to comply with the localization requirement is revealed during the announced audit, an access to Twitter can be blocked in Russia.

Observations – According to the regulator, Twitter is going to localize Russian citizens' personal data within the territory of the Russian Federation by the mid-2018.

Other key developments

Enforcement trends – The regulator is employing a risk-oriented approach in supervision of compliance with personal data regulations, opposite to the existing approach to plan audits for a whole year with no target on those processors most likely to breach personal data privacy regulations.

Sector focus – Education, e-commerce, medical and financial services, travel agencies, social networks, and recruiting and real estate agencies.

Litigation

Legal overview

Claims that may be brought by individuals

The Civil Code of Russia, data protection and employment laws set major requirements for privacy, data processing and data localization. These requirements are enforced, inter alia, through provisions on liability set by civil law (breach of confidence, defamation), the Code on administrative offences (data protection laws, employment laws) and the Criminal Code (misuse of private information).

The following cause of action are available for individuals to bring claims:

- Breach of data protection laws;
- Breach of confidence;
- Misuse of private information;
- Defamation; and
- Employment laws.

Key questions

What is the largest award of damages to date?

500,000 Russian rubles*

*Information from open sources. Full statistics are not available. In most cases an amount of granted damages is hidden.

<i>Can damages be obtained for non-financial loss?</i>	Yes
--	-----

<i>Can claimants bring class actions?</i>	No
---	----

No. Class actions can be brought by the regulator or public prosecution office only.

<i>Have they been used for data protection claims?</i>	Yes
--	-----

<i>Are "no-win-no-fee" arrangements available?</i>	Yes
--	-----

<i>Is third party litigation funding available?</i>	Yes
---	-----

What are the barriers (or perceived barriers) to litigation?

Insignificant amounts of damages awarded by the courts. Reimbursement of legal fees to a claimant is limited by courts to so-called 'reasonable amount' that is far from real expenses incurred by him/her.

Notable cases

Claimant(s): V Kontakte LLC

Defendant(s): Double LLC

Industry – Online technology and telecoms

Causes of action – Infringement of exclusive right to a database.

Significant points of law – Correlation between database rights and use of personal data contained in a public database.

Judgment – A social network vk.com is a hardware and software system that contains several databases, including users' personal data database, and the claimant put much efforts in development of the database.

The defendant collects personal data from the social network for the purposes of conducting personal data analysis (including customer checks) for banks and other banking and finance organizations.

The defendant's actions are infringement of the claimant's database rights.

Damages – 15,000 Russian rubles (~214 Euro).

Other key developments

Sector-specific campaigns – Branches of foreign legal entities in Russia – In 2017, the regulator sent to all the branches not included in the register of controllers maintained by the regulator requests to clarify legal reason behind not filing information about the branch for inclusion in the register and, if no such reason exists, to submit respective information to the regulator as soon as possible.

Media interest – The media pays significant attention to investigations and enforcement actions of the regulator as well as to comments of its officials.

Privacy groups/lobbies – Russian business is interested in less strict control and easier ways to comply with data privacy regulations.



Evgeniy Gouk

+7 (495) 967-6000, ext. 4961
evgeniy.gouk@pwc.com



Artem Dmitriev

+7 (495) 967-6000, ext. 4315
artem.y.dmitriev@pwc.com

South Africa

National law

National law – The Protection of Personal Information Act No.4. of 2013 (“POPIA”) (commencement/enforcement date to be announced which will be followed by a one year transition period).

Currently, data protection is addressed on a limited basis through disparate pieces of legislation, the South African Constitution and the common law.

Regulator – Information Regulator.

Enforcement powers – The Information Regulator is responsible for:

- Providing education through promoting an understanding of POPIA’s conditions, undertaking educational programs, advising data subjects in the exercise of their rights and public and private bodies on their obligations to ensure the lawful processing of personal information;
- Monitoring and enforcing compliance with POPIA including: monitoring and reporting on any developments that may impact data protection (e.g. technological, legislative), and conducting assessments/audits of public and private bodies who process personal information);
- Consulting with interested parties;
- Handling complaints including the investigation of complaints, and dispute resolution (i.e. mediation/conciliation);
- Conducting research and reporting to Parliament on matters relating to the processing of personal information;
- Issuing codes of conduct; and
- Facilitating cross-border co-operation in the enforcement of data protection laws.

Penalties –

Law: The maximum financial penalty under South African law is R 10,000,000 per data breach.

Imposed: None to date. (The commencement date of POPIA is still to be announced).

Breach notification – Mandatory. Breach notification is required under POPIA for breaches involving the unauthorised access to personal information. Breach notification needs to be provided to the Information Regulator and affected persons.

2017 notable issues

Breakdown of enforcement action

Enforcement trends – None to date as POPIA is yet to be enacted.

Litigation

Legal overview

Claims that may be brought by individuals – Claims may be brought by individuals under any of the following:

- Data Protection Laws;
- Common law action for breach of right to privacy;
- Right to Privacy in terms of the South African Constitution;
- Employment Laws; and
- Rights to privacy in terms of medical schemes and medical law.

Key questions

Can damages be obtained for non-financial loss?	No
Can claimants bring class actions?	No
Have they been used for data protection claims?	No
Are “no-win-no-fee” arrangements available?	No
What are the barriers (or perceived barriers) to litigation?	

Financial – claimants being unable to afford litigation.



Ashleigh van Kerckhoven
+27732197421
ashleigh.vankerckhoven@pwc.com



Busisiwe Mathe
+27822103121
busisiwe.mathe@pwc.com

Turkey

National law

National law – Protection of personal data is regulated for the first time under Turkish Law with the recently enacted Law on the Protection of Personal Data numbered 6698. The provisions of the Law are similar to the EU Directive 95/46/EC to a great extent.

The following laws govern the regulatory enforcement regime:

- Law on the Protection of Personal Data;
- Regulation on Deletion, Destruction or Anonymization of Personal Data;
- Regulation on Data Controller Registry;
- Communiqué on Application Procedures and Principles to Data Controller; and
- Communiqué on Notification Requirement.

Regulator – Personal Data Protection Board.

Enforcement powers – The enforcement powers are monetary and imprisonment sanctions with a maximum penalty of 1,000,000 Turkish Lira.

Penalties imposed – The largest penalty to date was for an overall amount of 125,000 Turkish Lira. The maximum financial penalty is 1,000,000 Turkish Lira.

Breach notification – Mandatory.

In cases where personal data is acquired by others through unlawful means, the data controller should notify the related data subjects and the Board of such a situation without undue delay.

Sector-specific regulation

Online technology and telecoms, Health, Banking and Capital Markets are the main sectors which specifically regulate data breaches.

Regulator – The regulator is the Information and Communication Technology Authority, Banking Regulation and Supervision Agency.

Breach notification – There is no clause related to mandatory breach notification in those sector-specific regulations. In this sense, Law on the Protection of Personal Data will apply. Therefore, where a data controller detects data breach it should notify the related data subjects and the Board without undue delay.

2017 notable issues

Litigation

Legal overview

Claims that may be brought by individuals – Protection of Personal Data was recently enacted in Turkey so there is no settled practice on Litigation.

Data subjects can bring claims under data protection laws and related secondary regulations; breach of data confidentiality and misuse of private information, defamation, harassment and employment laws, criminal laws and civil laws.

Other key developments:

Media interest – To date there has been no litigation practice regarding data protection breach in Turkey. On the other hand, the media is highly interested in personal data protection in general, due to the new regulation in Turkey.

Privacy groups/lobbies – The International Investors Association (YASED) has a working group, which fully concentrate on Data Protection studies. It holds seminars and conferences on different data protection matters and they obtain opinion from their members on the legislation.



Nilgün Serdar simsek

+90 212 326 6368

nilgun.simsek@pwc.com

National law

National law – there is no general right to privacy for citizens under the UAE Constitution.

Federal Law No. 5 of 1985 (the Civil Code) provides that a person is liable for acts causing harm generally, which could include harm caused by unauthorized use or publication of personal or private information.

Further, under Article 378 of the Penal Code (Federal Law 3 of 1987), it states that the publication of any personal data which relates to an individual's private or family life is an offence.

The most comprehensive privacy law in the UAE is the Federal Decree Law No 5 of 2012 on Combating Cybercrimes (the "Cyber Crimes Law") which introduces a wide range of offences and penalties, whilst criminalizing the invasion of one's privacy and exposure of confidential information by electronic means.

Regulator – There is no dedicated Data Protection Regulator.

Enforcement powers – Since there is no Data Protection Regulator there are no enforcement powers, the courts would therefore have jurisdiction over this.

Penalties imposed – The UAE restricts such information being published unless there is a particular matter of public interest.

Breach notification – There is no mandatory requirement under UAE Federal Law to report data security breaches.

Data subjects based in the UAE, however, may be entitled to hold the entities in possession of their data liable under the principles of the UAE Civil Code for their negligence in taking proper security measures to prevent the breach, if such breach has resulted in actual losses being suffered by the data subjects.

Sector-specific regulation

Different laws can apply to different free zones.

Free zone law – The Dubai International Financial Centre ("DIFC") has the following data protection legislation (DIFC Data Protection Legislation):

- Data Protection Law Amendment Law;
- DIFC Law No.5 of 2012 (Data Protection Law, DIFC); and
- Data Protection Regulations Consolidated Version No.2 of 2012.

Regulator – Commissioner for Data Protection ("CDP") oversees enforcement.

Enforcement powers – The CDP conducts all reasonable and necessary inspections and investigations before notifying a Data Controller that it has breached or is breaching the DPL or any regulations (Article 33). If the CDP is satisfied with the evidence of the breach, the CDP may issue a direction to the Data Controller requiring it to:

- Do, or refrain from doing, any act or thing within such time as may be specified in the direction (Article 33(1) (a)), and/or
- Refrain from processing any personal data specified in the direction or to refrain from processing personal data for a purpose or in a manner specified in the direction (DPL, Article 33(1) (b)).

Penalties – Law: The data controller may be subject to fines and liable for payment of compensation (Article 33(4)).

Breach notification – Data Controllers (or Data Processors carrying out a Data Controller's function at the time of the breach), must inform the CDP of the breach as soon as reasonably practicable (DPL, Article 16(4)).

Free zone law – The Abu Dhabi Global Markets ("ADGM") has the Data Protection (Amendment) Regulations 2018.

Regulator – The Office of Data Protection is the independent data protection regulator for the Abu Dhabi Global Market.

The Office of Data Protection is based within the Registration Authority and is responsible for promoting data protection in ADGM, maintaining the register of Data Controllers, enforcing the obligations upon Data Controllers and upholding the rights of individuals.

Enforcement powers – Registrar's powers and functions include the powers to:

- Access personal data processed by Data Controllers or Data Processors;
- Collect all the information necessary for the performance of its supervisory duties;
- Prescribe forms to be used for any of the purposes of these Regulations; and
- Issue warnings and make recommendations to Data Controllers.
- Further the Registrar may require a Data Controller by written notice to:
- Give specified information; or
- Produce specified documents which relate to the processing of personal data.

Penalties – Law: The maximum fine payable for non-compliance with any direction of the Registrar is USD 25,000.

Breach notification – Data Controllers should inform the Registrar without undue delay, and where feasible, not later than 72 hours after becoming aware, in the event of any unauthorized processing (including loss or disclosure) of personal data.



Richard Chudzynski
+971(0)564176591
richard.chudzynski@pwc.com

National law

Enforcement powers – Federal Trade Commission (“FTC”). Under the FTC Act, the FTC is granted administrative cease and desist authority to investigate, provide rules, order injunctive relief, and assign civil and criminal penalties under Section 5, which bars unfair and deceptive acts and practices in or affecting commerce. To exercise its authority, the FTC heavily relies on its special investigative powers that create a compulsory process. Another tool used by the FTC empowers the Commission to require filings of annual or special reports or answers to specific questions asked by the agency, in order to obtain information about the organisation and its conduct, practices, management, and relationship to individuals.

Federal Communications Commission (“FCC”). The FCC is an independent agency created by Title 47 of the United States Code that regulates interstate and international communications by radio, television, wire, satellite, and cable. To enforce the Communications Act and the rules created by the FCC, the agency initiates investigations and resolves claims through alternative dispute resolution.

To begin an investigation, the FCC receives information through numerous types of sources, such as a whistleblower, and proceeds through a Letter of Inquiry (“LOI”). This LOI requires the recipient to provide answers and produce documents to the FCC. If violations are discovered, the FCC can propose a penalty through a Notice of Apparent Liability for Forfeiture, which may result in a fine. Additionally, the agency can impose a forfeiture through a hearing process or take other types of enforcement actions that do not result in financial penalties.

Department of Health and Human Services, Office of Civil Rights (“HHS” and “OCR”). Within HHS, the OCR is designated as the enforcing body of the HIPAA Privacy and Security Rules. To enforce these rules, the OCR may accept a complaint and will inquire with the covered entity to present information about the incident. If the complaint describes conduct that may be a violation of the criminal provisions of HIPAA, the OCR refers the complaint to the Department of Justice for further investigation. At the end of the OCR’s investigation, the case will be resolved by voluntary compliance, corrective actions, and/or a resolution agreement. If the covered entity’s corrective action is insufficient, the OCR may impose civil monetary penalties.

Breach notification laws: federal – Health Insurance Portability and Accountability Act (“HIPAA”). The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the HHS, and in certain instances, the media, to breaches of unsecured Personal Health Information (“PHI”). The rule also applies to business associates of the covered entities, vendors of personal health records, and the vendors’ third party service providers.

Notice must be provided without unreasonable delay, and in no case later than 60 days from discovery of the breach. The media must be informed if the breach affects more than 500 residents of a state or jurisdiction within the same reporting timeframe.

- **Gramm-Leach-Bliley Act (“GLBA”).** Security guidelines for the GLBA recommend financial institutions to implement a risk-based response program that includes notification procedures for customers.
- When a financial institution becomes aware of unauthorised access to sensitive customer information, the institution should conduct a reasonable investigation. If it is determined that misuse of information occurred, notification to customers should occur as soon as possible. During the investigation, if it can be determined which customers’ information was accessed, the notification may be limited to just those customers instead of all customers in the group.
- **Federal Information Security Management Act (“FISMA”).** This act requires federal government agencies to provide security protections for information systems and data collected. Per FISMA, the agency’s security plan must include procedures to detect, report, and respond to security incidents. The National Institute of Standards and Technologies is responsible for developing the standards and guidelines that all agencies are required to comply with.
- **Veterans Affairs Information Security Act.** Under this act, if a breach of sensitive personal information processed or maintained by the Veterans Affairs Secretary occurs, the Secretary must ensure an independent risk analysis of the breach be conducted to determine the level of risk. Findings must be reported to the Veterans Committee, and if the breach includes sensitive personal data of Department of Defense civilians or enlisted personnel, the Secretary must report the breach to the Armed Services Committees.

Breach notification laws: state – 48 of the 50 states, as well as Guam, Puerto Rico, the District of Columbia, and the Virgin Islands enacted legislation requiring private and governmental entities to provide notification to individuals in the event of a security breach involving personally identifiable information. Alabama and South Dakota are the only states that lack breach notification legislation.

Typically, each law includes what constitutes an incident or breach, what information falls under the purview of the law, who is required to comply, and the timing, as well as any exceptions, for reporting. 37 states and Guam also define a harm standard, which requires an analysis to determine if a breach occurred. Most states’ laws only cover electronic data; however, ten also recognise tangible data. The Virgin Islands, Guam, and eight states do not require escalated reporting, although the remaining states have reporting requirements to a government agency, the attorney general, and/or consumer reporting agencies.

Class Actions. The Federal Rules of Civil Procedure (“FRCP”) Rule 23 governs class actions within the United States’ federal courts. The rule details prerequisites that are required for class actions, which include (1) the number of plaintiffs is so great a joinder is impracticable; (2) there are questions of law or fact; (3) the claims are typical of the class, and; (4) the representation of the parties will adequately protect the entire class. For individuals to bring such actions in state court, the states must adopt rules similar to Rule 23 of the FRCP. State rules vary greatly, with some disallowing class actions altogether while others limit types of actions that may be brought in this manner.

2017 notable issues

Breakdown of enforcement action

Federal Trade Commission

Case	Penalty
Dish Network Corp	\$280,000,000
Blue Global Media, LLC.	\$104,000,000
Home Depot	\$25,000,000
Lenovo	\$3,500,000
Upromise	\$3,500,000
2017 total	\$467,347,500

Dish Network Corp.

The company must pay \$280 million to the US government and four states for placing over 55 million robocalls to consumers on the National Do Not Call Registry, marking what the FTC says is a record fine for telemarketing violations. The company knew its contractors, in many cases, were violating do-not-call laws and did nothing, showing little concern for compliance. The states initially sought more than \$23 billion in damages, but lowered the request following the initial phase of a non-jury trial held in 2016. Dish Network disagrees with the ruling, and plans to appeal it.

Blue Global Media, LLC.

The operators of a lead generation business settled charges for \$104 million, stating they misled consumers into completing loan applications, then selling those applications containing consumers' sensitive information to virtually anyone willing to pay. The organisation operated dozens of websites enticing consumers to complete loan applications that were then sold as "leads" to a variety of entities without regard for how the information would be used or whether it would remain secure.

Home Depot

In 2014, hackers were able to retrieve email and payment card information from over 50 million individuals via malware through a vulnerability in self-checkout terminals. In a new settlement with dozens of banks, Home Depot has agreed to pay an additional \$25 million in damages they incurred as a result of the breach. In addition to the settlement, the organisation also paid at least \$134.5 million in compensation to consortia made up of Visa, MasterCard, and various others since the breach. Based on court documentation, the total cost of the breach is nearing \$200 million, and is expected to rise considerably.

Lenovo

The technology company violated state consumer protection laws by pre-installing hidden adware, VisualDiscovery, on hundreds of thousands of new laptops, making them susceptible to hacking and allowing a third party to monitor consumers' online activities to tailor advertisements accordingly. The program caused pop-up ads to appear on the user's screen, and while only information about websites the user visited were transmitted, the program had the ability to access all of a consumer's sensitive personal information transmitted online, including login credentials, social security numbers, medical information, and financial and payment information.

Upromise

This membership reward service once again did not disclose to consumers the extent of its data collection procedures, and failed to comply with the FTC's order to get required privacy assessments following a 2012 order requiring the organisation to make clear and prominent disclosures about their data collection and use, and to obtain third-party assessments and certifications describing specific safeguards and their effectiveness in protecting consumers' personal information.

Class Action/State Litigation

Case	Penalty
Wells Fargo	\$142,000,000
Anthem	\$115,000,000
We-Vibe	\$3,750,000
2017 total	\$592,826,200

Wells Fargo

Wells Fargo paid \$142 million in settlements to the owners of 3.5 million unauthorised checking or savings accounts, credit cards, or lines of credit that were surreptitiously opened in their names between 2011 and 2015. Customers will be paid for out-of-pocket losses; the amount each customer will receive will vary based on how many unauthorised accounts were opened in their name, and the degree of their financial losses.

Anthem

Potentially through the use of stolen employee passwords, hackers accessed the largest health insurance company in the US's database containing the personal information of 79 million people, including names, social security numbers, addresses, and income information, resulting in hundreds of lawsuits for the organisation. Anthem settled the litigation for \$115 million. The money will be used to pay for two years of credit monitoring for people affected by the hack.

We-Vibe

Unbeknownst to its 300,000 customers, and without their consent, the smartphone-paired vibrator organisation, Standard Innovation, secretly collected and transmitted users' personally identifiable information, including the date and time of each use, the user's personal email address, selected vibration settings, heat sensitivity, and frequency of use to its servers in Canada when remotely linked to the user's partner's account. The vibrator maker will pay \$3.75 million to settle their privacy class action lawsuit, agreeing to stop collecting users' email addresses, and to update its privacy notices, calling the settlement "fair and reasonable."

U.S. Department of Health and Human Services Office for Civil Rights

Case	Penalty
Memorial Healthcare System	\$5,500,000
Children's Medical Center of Dallas	\$3,200,000
CardioNet	\$2,500,000
2017 total	\$22,293,000

Memorial Healthcare System ("MHS")

MHS paid HHS \$5.5 million to settle potential HIPAA Privacy and Security Rule violations, and agreed to implement a robust corrective action plan. MHS reported to the OCR that the protected health information of 115,143 individuals was impermissibly accessed by its employees, and impermissibly disclosed to affiliated physician office staff. Login credentials of a former employee of an affiliated physician's office were not appropriately revoked, and the employee was able to access electronic protected health information ("ePHI") maintained by MHS on a daily basis without detection.

Children's Medical

A pediatric hospital based in Dallas, was fined \$3.2 million based on its impermissible disclosure of unsecured ePHI and non-compliance of many standards of the HIPAA Security Rule over many years. Specifically, Children's Medical was fined for the failure to implement risk management plans and a failure to deploy encryption or an equivalent alternative measure on all of its laptops, workstations, mobile devices, and removable storage media despite knowledge about the risk of maintaining unencrypted ePHI on its devices as far back as 2007.

Cardionet

Settled potential noncompliance with the HIPAA Privacy and Security Rules by paying a \$2.5 million fine and implementing a two year corrective action plan to resolve a claim that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. The OCR revealed that CardioNet had insufficient risk analysis and risk management processes in place, and CardioNet was unable to provide any policies or procedures regarding ePHI safeguards. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

Federal Communications Commission

Case	Penalty
Adrian Abramovich & Co.	\$120,000,000

Adrian Abramovich

Adrian Abramovich and a group of companies used Internet Protocol (IP) technology to spoof phone numbers over a three month period. The group repeatedly made robocalls soliciting users to sign up for vacation packages without consumer consent. The robocalls interfered with an emergency paging service to page emergency room doctors, nurses, and other first responders. This enforcement action is the first under the Truth in Caller ID Act of 2009 and is alleged to be one of the most hazardous illegal robocalling scams ever recorded. The FCC characterised Abramovich's schemes as "one of the largest – and most dangerous – illegal robocalling campaigns the Commission has ever investigated."

Consent Decrees

Uber Technologies, INC.

Agreed to implement a comprehensive privacy program and obtain regular, independent audits for the next 20 years to settle FTC charges alleging the ride-sharing company deceived consumers by failing to monitor employee access to consumer personal information, and by failing to reasonably secure sensitive consumer data stored in the cloud. In its complaint, the FTC alleged that Uber failed to live up to its claims that it closely monitored employee access to consumer and driver data and that it deployed reasonable measures to secure personal information stored on a third-party cloud provider's servers.

Labmd, INC.

In a still undecided case, beginning with the FTC's initial complaint filed in 2013, the US Court of Appeals for the Eleventh Circuit heard another series of arguments from both parties in 2017. As a brief background, in 2013, the FTC argued LabMD, who is no longer in operation, failed to reasonably protect the security of consumers' personal data and sensitive medical information, which was exposed on a peer-to-peer file-sharing network. The complaint alleged LabMD's lax data security standards caused or were likely to cause substantial injury to consumers.

The crux of LabMD's argument is that purely conceptual privacy or security harm does not constitute "substantial injury" within Section 5 of the FTC Act. The FTC looked to US common law to define "substantial injury," arguing that individuals unaware they have suffered an injury does not mean an infraction has not occurred. No decision has been issued since the close of 2017, but the Eleventh Circuit's ruling will have far-reaching implications, potentially helping to define the scope of the FTC's power to enforce its Section 5 authority in matters of cybersecurity and privacy, requiring actual harm opposed to hypothetical, and treating past consent decrees as precedent as to what is seen as "unfair or deceptive" practices from a cybersecurity standpoint. For those with a legal background, any general interest in legal cybersecurity proceedings, or a curiosity on what the legal process entails in the US once an organisation is hit with a privacy or security lawsuit, the June 2017 oral argument (available online via the Eleventh Circuit's website) is highly entertaining.



Jay Cline
+1 (612) 596 6403
jay.cline@pwc.com



Daniel Pomierski
+1 (312) 298 5583
daniel.pomierski@pwc.com



Kelly Villanueva
+1 (312) 596 9753
kelly.m.villanueva@pwc.com



Lana Bonadeo
+1 (312) 298 3940
lana.bonadeo@pwc.com

An aerial photograph of a city street scene. In the top left, a couple walks. A woman walks alone in the center. A cyclist is in the top center. Two people walk on a sidewalk to the right. In the bottom left, a group of people is gathered around a black sculpture. A white bus is visible in the bottom right corner. The background is a mix of paved areas, sidewalks, and some greenery.

Take our GDPR C.A.T. (Completeness Assessment Tool)

Targeted assessment of an organisations levels of maturity with the provisions of the GDPR to enable any areas of weakness to be identified and effective remediation plans defined.

- 1 taxonomy
- 2 domains – architecture and principles
- All GDPR articles & recitals
- 70+ questions
- 1 maturity matrix
- 1 benchmark
- 2 heatmaps
- 2-3 hours

For further information please contact DP_Enquiries@uk.pwc.com



Team and Contact Information

Co-Global Data Protection Leaders



Stewart Room

Global Head of Cyber Security and Data Protection
Legal Services; UK Data Protection National Leader
+44 (0)7711 588978
stewart.room@pwc.com



Jay Cline

Co-Global Leader, USA Data Protection Leader
+1 (612) 596 6403
jay.cline@pwc.com

PwC UK Data Protection Leaders



Andrew Paynter

Partner, Data Protection Assurance Leader
+44 (0)7802 788403
andrew.paynter@pwc.com



Mike Greig

Partner, Data Protection Consulting Leader
+44 (0)7706 655716
mike.greig@pwc.com



Umang Paw

Partner, Data Protection Forensics Leader
+44 (0)7931 304666
umang.paw@pwc.com



Chris Reeve

Partner, Data Protection Tax Leader
+44 (0)7764 903058
chris.a.reeve@pwc.com

Directors



Jane Wainwright

Director
+44 (0)7715 034015
jane.a.wainwright@pwc.com



James Drury-Smith

Director
+44 (0)7841 803538
james.drury-smith@pwc.com



Kate Macmillan

Director
+44 (0)7718 979744
kate.macmillan@pwc.com



Fedelma Good

Director
+44 (0)7730 598342
fedelma.good@pwc.com

Senior Managers



Brian Davidson
Senior Manager
+44 (0)7710 037412
brian.j.davidson@pwc.com



Hilary Coote
Senior Manager
+44 (0)7710 036862
hilary.coote@pwc.com



Jane Foord-Kelcey
Senior Manager
+44 (0)7525 897862
jane.foord-kelcey@pwc.com



Mária Roman
Senior Manager
+44 (0)7843 334691
maria.roman@pwc.com



Mark Hendry
Senior Manager
+44 (0)7715 487457
mark.hendry@pwc.com



Polly Ralph
Senior Manager
+44 (0)7843 332567
polly.ralph@pwc.com

Managers



Sean Milford
Manager
+44 (0)7710 036856
sean.milford@pwc.com



Craig Fyfer
Manager
+44 (0)7701 297345
craig.m.fyfer@pwc.com



Emily Sheen
Manager
+44 (0)7561 788941
emily.sheen@pwc.com



James De Cort
Manager
+44 (0)7710 035635
james.de.cort@pwc.com



Samantha Sayers
Manager
+44 (0)7841 803730
samantha.sayers@pwc.com



Sarim Shaikh
Manager
+44 (0)7706 284810
sarim.s.shaikh@pwc.com

Senior Associates



Lucy Tucker
Senior Associate
+44 (0)7843 370254
lucy.c.tucker@pwc.com



Sara Jameel
Senior Associate
+44 (0)7718 978175
sara.e.jameel@pwc.com



Tamsin Hoque
Senior Associate
+44 (0)7718 978782
tamsin.h@pwc.com



Tannia Khan
Senior Associate
+44 (0)7764 958673
tannia.khan@pwc.com



Olivia Wint
Senior Associate
+44 (0)7710 035127
olivia.wint@pwc.com



Simon Davis
Senior Associate
+44 (0)7706 285054
simon.y.davis@pwc.com



Cátia Reis
Senior Associate
+44 (0)7561 788948
catia.c.reis@pwc.com



Kayleigh Clark
Senior Associate
+44 (0)7841 468403
clark.kayleigh@pwc.com



Lewis Brady
Senior Associate
+44 (0)7802 660495
lewis.w.brady@pwc.com



Richard Collinson
Senior Associate
+44 (0)7802 659192
richard.j.collinson@pwc.com



Tughan Thuraisingam
Senior Associate
+44 (0)7702 699288
tughan.thuraisingam@pwc.com

Associates



Ali Sheikh
Associate
+44 (0)7843 370254
ali.sheikh@pwc.com



Jordyn Pankhurst
Associate
+44 (0)7718 978175
jordyn.pankhurst@pwc.com



Rima Karia
Associate
+44 (0)7841 468299
rima.karia@pwc.com

Support staff



Oihana Altube
CA
+44 (0)7710 035881
oihana.altube@pwc.com



Tara Nash
PA
+44 (0)7702 698615
tara.nash@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2018 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

180501-103905-JP-OS