Legal Academy

February 2023

pwc

Data Protection – the regulatory landscape, key trends, challenges, and preparing for upcoming changes

PwC Data protection legal team

Our team advises clients on the laws and regulations in relation to personal data. Much of our work originates outside the UK, advising clients with global operations in connection with issues such as **GDPR compliance, international data flows and cross-border transfers**. We also advise in the case of serious data breaches and other **crisis management** situations, provide **thought leadership on emerging issues,** such as **the use of AI**, and how to incorporate **privacy by design** into new services and business models.

Orla Middlemiss
Manager
orla.middlemiss@pwc.com

Orla recently joined PwC permanently following a secondment from the UK Government's Department of Digital, Culture, Media and Sport where she was a Senior Adviser on Data Policy.

During her time in the public sector, Orla helped to design the UK's new international data transfers framework, and has also worked at the Information Commissioner's Office where she has experience assessing organisational compliance with UK data protection law.

Lucas Saric
Senior Associate (Solicitor)
lucas.saric@pwc.com

Lucas is a solicitor in the Data Protection team (part of Legal Business Solutions) at PwC UK. He holds the CIPP/E qualification and is a certified OneTrust Professional. He also leads the PwC UK partnership with Aspiring Solicitors aimed at increasing diversity within, and enabling wider access to, the legal profession.

Agenda

UK & EU Privacy Regulatory landscape 1

Case Study 1: Transitioning to the cloud 2

Case Study 2: Diversity Reporting (ESG) 3

Regulatory pipeline 4

Key takeaways 5

Questions 6

Poll question

What is your current level of data protection experience / knowledge?

- No experience or knowledge – help!
- Some experience, but very basic knowledge.
- Data protection considerations are a regular component of my work.
- Data protection is the focus of my job, and I am well versed in the data protection issues faced by organisations.

UK & EU Privacy regulatory landscape

1

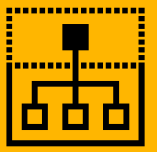
Laws that governs the processing of personal data (i.e. any data relating to living individuals).

2

Apply to all sectors in the economy and all sizes of business with the aim of protecting the rights and freedoms of individuals.

3

In the UK the framework is regulated and enforced by the ICO. The maximum penalty for breaches is £17.5mn or 4% of total annual worldwide turnover.



4

Territorial scope – the UK and EU GDPR have g
reach, regardless of whether or not the processing of data takes place within the UK or EU.

UK & EU Privacy regulatory landscape

Key legislation	
EU General Data Protection Regulation (EU GDPR)	• EU-wide principles-based data protection legislative framework. • Strong focus on the rights of individuals (data subjects) and high threshold for organisations to demonstrate accountability. • **Scope:** Applies to organisations operating in the EEA, offering good or services in the EEA or monitoring the behaviour of people in the EEA.
UK General Data Protection Regulation (UK GDPR)	• Mirrors the EU GDPR; adopted post-EU exit with minor practical amendments. • **Scope:** Same as EU GDPR, but replace 'EEA' with 'UK'.
Data Protection Act (DPA) 2018	• Implements the GDPR in the UK. • Sets out a separate regime for law enforcement authorities and for intelligence services.
ePrivacy Directive 2002	• EU directive on data protection and privacy in the digital age. • Complements the wider privacy framework (including GDPR) by setting out more specific rights and rules about the use of electronic communications. This includes use of cookies and other tracking technologies, marketing by electronic means (including calls, text and emails), and the security of communications services.
Privacy and Electronic Communications Regulations (PECR) 2003	• Implements the ePrivacy Directive in the UK. • Regulated by the ICO.

What is personal data?

Personal data


Name and id Number

IP address

GPS

Special categories of personal data



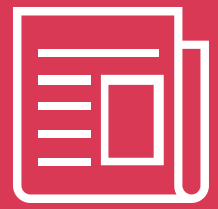

Race **Religion** **Political beliefs** **Trade union**



Health **Genetic** **Biometric**


Sexual orientation **Sex life**

- Personal data is any information that may directly or indirectly identify a living individual, who is called a data subject.
- There are also Special Categories of Personal Data which are afforded additional protections under the GDPR.
- Personal data relating to criminal convictions and offences should also be treated as ‘sensitive’.



Data Protection Principles and Rights

Principles

1st – Data must be processed data fairly, lawfully and transparently

2nd – Data can only be obtained and processed for ‘specified, explicit and legitimate purposes’

3rd – Data should be ‘adequate, relevant and limited to what is necessary’

4th – Data should be ‘accurate and, where necessary, up to date

5th – Data that is no longer needed must be removed

6th – Data must be handled in a manner ensuring appropriate security

7th – Organisations must be able to demonstrate their compliance with the legislation (accountability)

Data protection principles and rights

Data Subject (Individual) Rights

The rights are not absolute and there are exemptions to them.

Right to be informed

Right of access

Right to rectification

Right to erasure

Right to restrict processing

Right to data portability

Right to object

Poll question:

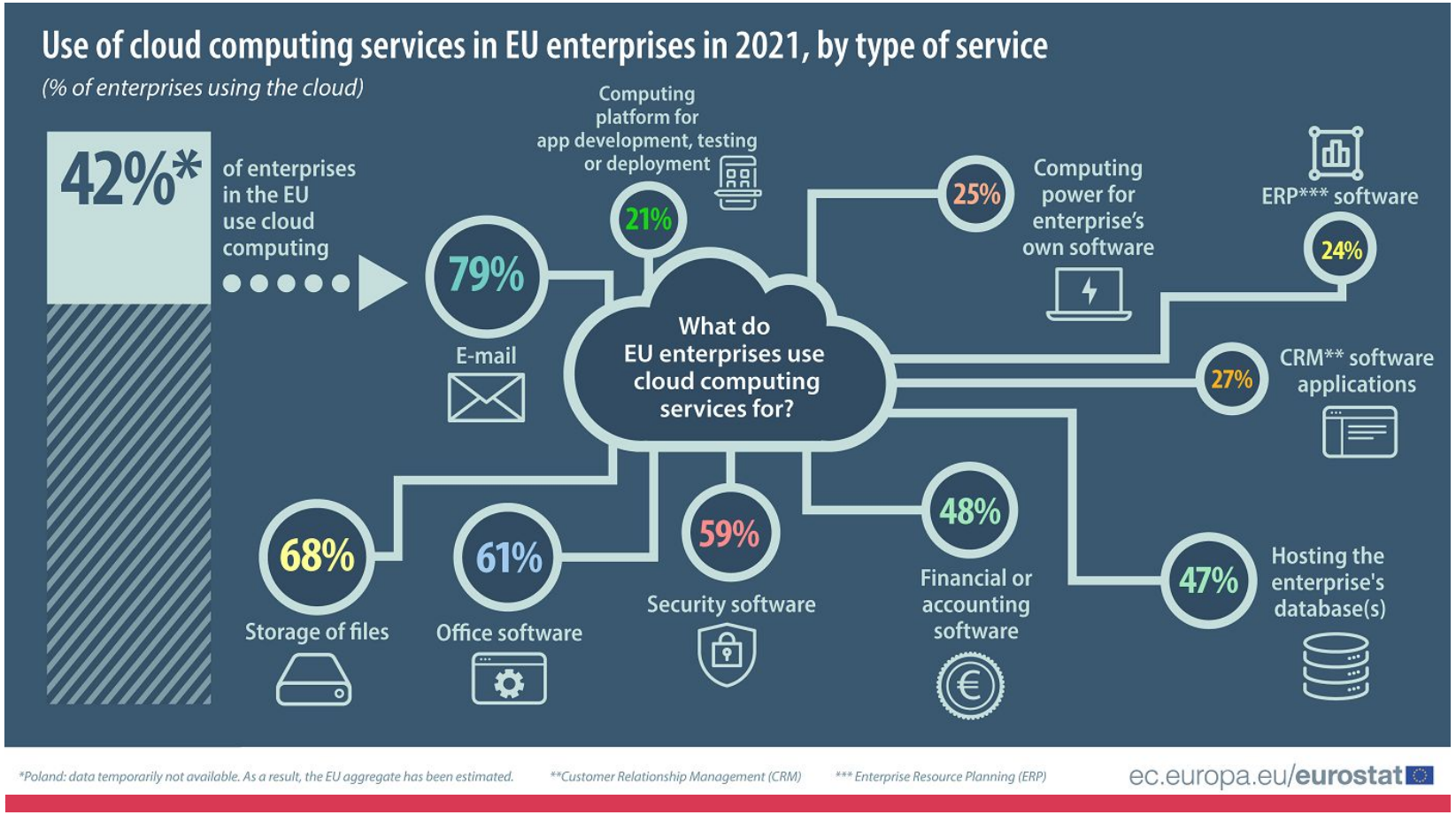
Does your business use cloud service providers / cloud computing (e.g. AWS, Azure, Oracle)?

- Unsure.
- No.
- Not currently but there are plans to in future.
- Yes.
- Yes and plans to expand further.

Case Study 1: Transitioning to the cloud

Context:

Cloud services are intrinsically data-based services. They deliver computing services over the internet. They have been widely adopted by businesses across the economy and now underpin many of the services that businesses and consumers rely on in a day-to-day basis. The nature of cloud technologies means that their use by businesses introduces particular data protection and privacy considerations. The top providers include Amazon Web Services, Microsoft Azure, Oracle Cloud, and Alibaba Cloud.



Case Study 1: Transitioning to the cloud (continued)

Scenario

A UK based Bank is looking to migrate key business operations to the cloud in order to leverage AI and machine learning capabilities to perform advanced data analytics.

It wants to build privacy considerations into the design, testing and rollout to reduce potential privacy risks.

Data Protection Considerations

Impact Assessment

Data Protection Impact Assessment required to comply with accountability obligations.Mitigates impacts and risks.

International transfers

Data mapping to determine where data is going to be stored and whether a mechanism, such as International Data Transfer Agreements, is needed.

Contracts

Contract required between data controllers (you) and data processors (cloud providers).
GDPR sets out what needs to be included.

Security

Due diligence checks required on potential providers to identify whether additional security measures need to be implemented.

Transparency

Work may be required to update private notices, consent statements and other documents to ensure they remain compliant.

Audits

Agreed ongoing monitoring of cloud provider's adherence to specified data protection obligations is required.

Regulatory / complaints

Roles and responsibilities under contract with provider as to engagement with regulator / s and complaints management.

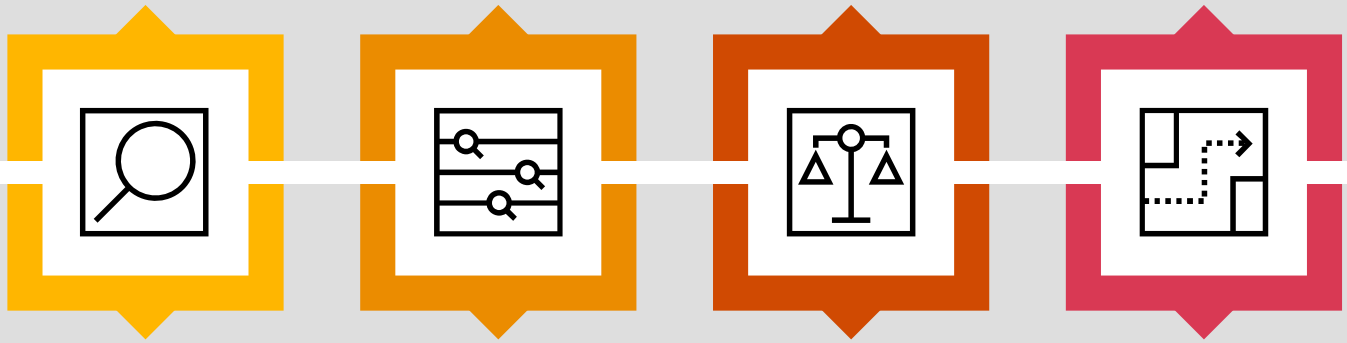
Case Study 2: Diversity data collection and analysis (ESG)

This diagram sets out the key stages in a typical diversity data collection exercise. The scope and complexity of each step will be influenced by the type of data collected.

In your breakout groups, consider the following questions:

- How does the collection of diversity data for reporting purposes align with data protection principles?
- How will you collect this data?
- What will you tell individuals?
- How will you protect the data?
- How will you share the data?

?



1: Identify scope, key priorities and desired outcomes.

2: Review of Permissibility.

3: Detailed legal and privacy analysis.

4. Analytics and reporting.

Breakout session

Case Study 2: Diversity data collection and analysis

	Privacy Considerations
1: Identify scope	What data is being collected? (E.g. Is special category data covered? Are we collecting the minimum amounts of data required for the purposes of reporting? Develop key project objectives / purpose and milestones, along with key measures of success. (E.g. What benefits will arise from this initiative? Clear objectives should be given to respondents when asking for their consent). Will a DPIA be required?
2: Review of permissibility	Are consent requirements met (especially when considering sensitive data)? If existing data is being repurposed then is fresh consent required from individuals? Conduct territory-specific legal reviews to identify specific steps needed to comply with employment and data privacy law in other jurisdictions.
3: Detailed legal and privacy analysis	Consider the other data protection principles and what obligations they put on the data processor / controller. (E.g. How will access to data sets be restricted to key personnel (data security principle)? How long does data need to be retained for, what mechanisms are in place to remove / anonymise data when necessary (storage limitation principle)? Draft / update appropriate documentation for each territory. This might include: • Consent documentation. • Updated privacy notices. • Data Protection Impact Assessments.

Case Study 2: Diversity data collection and analysis (continued)

	Privacy Considerations
4. Analytics and reporting	Build dashboards to allow data sharing and investigation in line with data privacy requirements: Privacy by design and default. Purpose limitation: ensure all data collected for these purposes are only used for the stated purpose. Consider additional requirements if needed for other purposes. Data Subject Rights: This information will be subject to various data subject rights, including Access requests (DSARs), so having a clear understanding of what data is held, and where it is held is critical to reduce administrative burden.

Regulatory pipeline – what is on the horizon

EU digital services package

EU Digital Services Act

- Regulates provision of digital intermediary services.
- Introduces new obligations and prohibitions, e.g. relating to targeted advertising and dark patterns.

EU Digital Markets Act

- Imposes obligations (including data and interoperability rules) on 'gatekeeper' platforms.
- Gatekeepers are providers of core platform services that meet certain financial and user thresholds.

UK

UK Data Protection and Digital Information Bill

'Updating and simplifying the UK's data protection framework and the role of the Information Commissioner's Office (ICO) while focusing on protecting individuals' data rights and generating societal, scientific, and economic benefits.

Other pipeline regulations

- UK Online Safety Bill.
- Product Security and Telecommunications Infrastructure Bill.
- Digital Markets Competition and Consumer Bill.

EU data strategy and artificial intelligence strategy

EU Data Governance Act

- Establishes a governing framework for data sharing and uses in the EU.
- Regulates the re-use of public data, data intermediation services and data altruism activities.

EU Data Act

- Applies to manufacturers of smart devices and cloud services providers.
- IoT products have to allow users to easily and in real time access data collected or generated.

EU Artificial Intelligence Act

- Covers providers, manufacturers, users, distributors and importers of AI systems.
- Bans certain AI systems and requires a conformity assessment with respect to high-risk AI systems.

Key Takeaways

1. **Compliance with data protection regulations needs to be considered from the perspective of every data subject.** It is not only customers or clients, but also your employees, contractors, job applicants, suppliers, visitors etc. that your organisation is required to comply with the data protection principles and rights.

2. **Ensure you have a clear understanding of your / your team's role and responsibilities.** Where is the handoff between the role of the Data Protection / Privacy Office / Information Governance teams etc.? E.g. in the event of a data breach or regulatory investigation, or when entering into contracts with new vendors / service providers?

3. **Take a Privacy by Design approach** to the introduction of new systems, procedures, services, or processes. Factoring in privacy considerations (such as including relevant data provisions within contracts and service agreements) at as early stage as possible greatly reduces cost, time and risk.

4. **Keep up to date with upcoming changes.** The ICO publishes a monthly newsletter and PwC also produces a wider Monthly Legal Newsletter for clients that will include relevant privacy content and updates from time to time. We also have a series of blogs and articles published that you can access online, some of which are linked below.

Resources:

- The UK DPDI Bill: Changes Impacting Accountability, Changes Impacting PECR, Changes Impacting the ICO.
- ICO newsletter.

Poll question:

What follow-up to this webinar do you think you'll undertake?

- Download slides post-webinar and review when needed.
- Sign up to ICO newsletter and / or read other resources flagged.
- Consider data protection more readily in day-to-day role.
- All of the above.

Your feedback matters

Thank you

pwc.com

RITM11302505