October 2017

Technology's role in data protection – the missing link in GDPR transformation

pwc

Sponsored by MICRO FOCUS

Contents

Executive summary

The EU General Data Protection Regulation (GDPR) delivers a fundamental change in how data controllers and data processors handle personal data. Instead of an 'add-on' or afterthought within business operations, protections for personal data will now have to be designed into the very fabric of data processing systems, meaning that entities will need to re-examine how they approach the use of technology in their organisations.

European data protection law has always been concerned with how technology operates. Indeed, the first proposals for harmonised, pan-European laws were a response to technological developments. Legal instruments such as Council of Europe Recommendation 509 on human rights and modern scientific and technological developments (31 Jan. 1968) pinpointed with precision the risks to privacy that were posed by the technology revolution of the 1960s. Data protection laws exist because it is believed that, without them, technology will enable or cause data controllers and processors to trample on fundamental rights and freedoms.

Technology is, in other words, the principal problem that data protection law is trying to solve. As such, it is obvious that, as well as being the problem, technology must provide the solution. If entities are storing too much personal data, for example, technology needs to deliver delete, erase, de-duplication and minimisation functionality.

However, the way that data protection has operated in practice tells a different story and PwC's experience in this area backs this up: despite technology being both the problem and the solution, technology systems have not been designed and deployed from the perspective of the requirements of data protection law. This is why we see so much debate over the retention and storage of personal data, so much confusion about the nature and whereabouts of personal data and so many technology-related cyber-security failures. From this perspective it might be said that the technology stack has been the missing link in data protection programmes over the years.

The underlying reasons for these issues will no doubt continue to be a source of debate, but one thing is certain: in the new world of the GDPR, where tougher and more penetrative forms of adverse scrutiny are likely, instances of technology failure will be harder to excuse.

The principal contention of this White Paper is that data controllers and processors who are engaged in the design, build and delivery of GDPR programmes should re-examine and rebalance their priorities, in order to deliver the best possible technology environment for personal data before the GDPR comes into force in May 2018. As part of this rebalancing exercise, they should:

- Critically examine whether they have enough time, space and resources in their programmes to deliver what is required in their technology stacks by May 2018. As part of this process they should consider performing a technology functionality gap analysis, whereby the operational performance of technology is tested against the requirements of (1) the data protection principles, (2) the data subject rights and (3) the programme build requirements described in the GDPR.
- Perform a risk and cost-benefit analysis, whereby the operational risks to personal data and the legal and reputational risks to the controller or processor of data protection failure are weighed against the 'feasibility issues' associated with delivering technology change, such as the lead time required to source, procure, install and test new technology. Central to this exercise is an understanding of the nature of the technology market and the consensus of professional opinion on what 'good' looks like.

In weighing up the options, controllers and processors should bear in mind that, for the first time, data protection law now contains real incentives for the delivery of technology change. As well as the obvious risk of regulatory enforcement action, including the risk of sizeable financial penalties, there is a new 'litigation risk' built into the GDPR, all underpinned by transparency mechanisms that will shine a spotlight on what is actually happening to personal data, including when security fails.

Conversely, there are also significant gains to be made from taking a 'good' approach to the technology issues. Issues such as efficiency and productivity gains are not new to data protection, but we are also now seeing a stronger focus on data protection in B2B procurement and contractual processes. Businesses and their contracting partners are starting to ask more penetrative questions about technology, meaning entities with a good story to tell will perform better in a competitive market. Likewise, consumers will increasingly factor-in data protection issues when choosing where to place their business.

'1995 was a long time ago. In terms of technology, a different age'

Since 1995 'the internet has blossomed, social networking has boomed, cloud computing has taken off, and these changes have fuelled an explosion in data process'.

Announcing her vision for EU data protection reform, Viviane Reding, former vice president of the European Commission, said data protection must deal with constant technological change, more so than many other legal areas, and that advances in technology since the 1995 Data Protection Directive had overridden individuals' rights.

1. *Viviane Reding, The overhaul of EU rules on data protection: making the single market work for business, 04.12.2012;*
2. *Seven basic building blocks for Europe's privacy reform, 20.03.2012;*
3. *A data protection compact for Europe, 28.01.2014.*

Stewart Room
Partner, PwC UK

Joint Global Head of Data Protection;
Global Cyber Security and Data Protection Leader;
UK Data Protection Leader

Mobile: +44 (0)7711 588978
Email: stewart.room@pwc.com

Responding to the fear of technology – why data protection law exists

The first versions of European data protection law emanated from the Council of Europe, as part of its human rights agenda. It is immediately obvious from their titles that these laws were passed in reaction to a fear of the intrusive power of technology. A 1968 Council of Europe Recommendation talks about 'serious dangers for the rights of the individual inherent in certain aspects of modern scientific and technological development', for example. It went on to describe the technologies causing these dangers as including 'phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda'.

In many respects, the concerns of 2017 are the same as those of 1968. Fears about phone-tapping and eavesdropping played out dramatically in Edward Snowden's disclosures about mass surveillance by intelligence agencies, and contributed directly to the collapse of the EU-US Safe Harbour data transfer agreement, fears about surreptitious observation regularly arise in official warnings about the use of CCTV systems from European data protection regulators, and fears about subliminal advertising and propaganda surface in the regulatory agenda about profiling-backed direct marketing.

These fears can be seen as a thread running through all of the legal developments since 1968, such as the Council of Europe Data Protection Convention 1981, the EC Data Protection Directive 1995, the EC Telecommunications Data Protection Directive 1997, the Privacy and Electronic Communications Directive 2002–2009, and the Data Retention Directive 2006. The GDPR now continues and sharpens this focus on technology.

Transition to the GDPR – technology under heightened scrutiny

The GDPR's focus on technology is much more explicit than its predecessor, the Data Protection Directive. If it is to be properly effective, however, the GDPR must assist in the delivery of business transformation and legal compliance. It does this in a number of ways. It requires the use of Privacy by Design techniques and the performance of risk assessments. It also identifies data management techniques, such as data mapping, and techniques for how to handle operational failure, such as breach disclosure.

Technology goal #1

Driving data protection principles into technology, through appropriate technical and organisational measures

The data protection principles set out the core compliance goals of the law. They have been at the heart of European data protection regulation from its very beginning in the 1960s. The principles must be delivered in the technology stack and organisations must take 'appropriate technical and organisational measures' to do so. When developing those technical and organisational measures, organisations must have full regard to the 'nature, scope, context and purposes of processing' and 'the risks of varying likelihood and severity for the rights and freedoms of natural persons'. The obvious implication of this requirement is that risk assessments must be performed in all cases. These risk assessments require a deep understanding of the effect that technology can have on individual rights and freedoms.

Technology goal #2

Ensuring the technology environment can protect individuals' rights

If people are to have control over their personal data, they need rights over that data and transparency about what is happening to it. But the exercise of these individual rights is only truly effective if an organisation's technology stack is fully responsive to them, and has the right functionality embedded in it.

The core individual rights are the 'right of access', 'right to rectification', 'right to erasure' (or the 'right to be forgotten'), 'right to restriction of processing', 'right to data portability' and 'right to object'. In a functional sense, these rights require the technology to:

- Connect individuals to their personal data;
- Categorise personal data by type and processing purpose;
- Map or trace the full information lifecycle;
- Perform search and retrieval;
- Enable rectification, redaction, erasure and anonymisation;
- Enable freeze and suppression;
- Enable the transmission of personal data from one technology stack to another.

All of this must be protected by appropriate security.

Technology goal #3

Adopting a proper approach to technology design and deployment

One of the GDPR's innovations is the inclusion of requirements that provide organisations with practical assistance in how to flow data protection into technology. These are:

- Accountability;
- Records of processing activities;
- Data protection by design and default;
- Data protection impact assessments;
- Breach notification.

Collectively, these new requirements provide a 'user manual' for delivering operational success.

Article 24 (1) – Responsibility of the controller

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Accountability – proving that technology works properly

The key idea within accountability is that organisations will be able to demonstrate that their technical systems operationally adhere to data protection principles and citizen rights. It will require organisations to maintain a repository of the functional requirements of their technology systems. They will also need to demonstrate how those requirements are delivered through associated design, plans, functional testing and assessment documentation. Accountability also means that the technology must be properly tested for operational quality.

Records of processing activities – understanding the data lifecycle and what technology does

The delivery of the principles and rights in the GDPR will not be possible if an organisation does not have a complete understanding of its personal data and its processing activities. The GDPR tackles this head on, requiring organisations to maintain records of: the categories of individuals whose data are processed, the categories of data that are processed, the categories of recipients of the data and their geographical whereabouts, the retention periods that apply to the data, and the security measures that have been applied. These records will be disclosable to the regulators on request.

There are many techniques that can be deployed to understand the data lifecycle, but the challenge that many organisations are now grappling with is that their technology has not been designed to deliver the required information. In an attempt to get around this technology problem, many organisations are trying to build 'data maps' manually, through question and answer sessions with personnel. The problem with this approach is that it can be very labour intensive, disruptive to the daily life of business and is rarely complete and accurate. For these reasons alone it makes sense to look for technology solutions, such as software that can identify and categorise different types of data and track its use and flow. The data protection by design and default requirement supports this outcome.

Data protection by design and default – getting technology right from the start

Data protection by design and default (sometimes called 'privacy by design' or just 'PbD') is another innovation of the GDPR. The problem that PbD sets out to solve is a lack of forethought by organisations when they start to collect personal data. Far too often data protection is an afterthought, and PbD brings data protection thinking forward to a much earlier stage in the data processing continuum. It requires organisations to think through data protection issues during the planning phases for data processing. As such, PbD begins when data processing activities are still in a theoretical state.

The idea of the data protection by default component of PbD is that data processing systems should process only the minimum of amount of personal data required to deliver the processing purpose. This is about not only placing limitations on the types and volume of personal data that are processed, but also reducing the number of times that processing occurs, reducing the retention period for the data and reducing the number of people, the number of entities and the number of technology systems that can access the data.

PbD requires organisations to be intimately familiar with the way their technologies operate and with the ways that technology can be redesigned, reconfigured or replaced to deliver fewer and better data processing operations. Clearly, this has implications for legacy systems which have never been considered from a data protection perspective.

Data protection impact assessments – understanding technology risk

There is a significantly increased focus on risk management in the GDPR. Before an organisation can make decisions about the technical and organisational measures it should adopt for data protection, it needs to understand the data protection risk posed by its data processing activities and the wider environment in which it operates. In special cases, the GDPR requires a special form of risk assessment, called a data protection impact assessment (DPIA), which is needed when the processing activities are 'likely to result in a high risk to the rights and freedoms of natural persons'. The legislation points out that these risks can emerge when 'using new technologies'. Such risks might arise, for example, during the profiling of individuals (as happens in the insurance sector, or in the retail sector for the purposes of behavioural advertising), during large-scale processing of personal data (as may happen in large clinical trials in the health sector, or in criminal justice) and through large-scale systematic monitoring of public places (as may happen with CCTV and other public surveillance systems).

In looking at the trigger points for DPIAs, like the reference to 'new technologies' and likelihood of 'high risks', it becomes obvious that GDPR programme owners need to be intimately familiar with the nature of their organisations' technology stacks and how they operate. Those programme owners need to be plugged into the technology refresh and upgrade cycles, so they can capture anything new within their methodologies.

Breach notification – delivering transparency in technology failure

The long history of security breach failures has crystallised the need for mandatory breach notification in Europe. Under these rules, data controllers have to inform the regulators of any personal data breaches without undue delay, and certainly within 72 hours of becoming aware of a breach, while data processors must notify controllers. In cases where a personal data breach is likely to result in a high risk to the rights and freedoms of people, the controller needs to notify those persons, again without undue delay.

The security principle, and the requirement for appropriate technical and organisational measures, combines with the rules on breach notification to require technology that can prevent breaches from happening, detect them when they do happen, and help with the restoration of systems and handling after they happen. GDPR requires end-to-end security.

On the prevention side, the GDPR contains obligations for 'regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing'. On the breach notification side, the rules require notification of the nature of a breach, the volumes of data and people affected, information about the likely consequences, and measures taken to address the breach and mitigate harm. All this information should be recorded in a register of breaches, which is a disclosable document.

Again, these rules demonstrate the need for the GDPR programme to operate effectively inside the technology stack.

Conclusions for technology – bridging risk management, functionality and data management

Looked at in this way, the GDPR's requirements for technology are about risk management, functionality and data management. These are the three pillars on which data protection law for technology is built. If any individual pillar is overlooked, the organisation will be at peril of operational and legal failure. Organisations should ask themselves whether their GDPR programmes are properly addressing these requirements in technology.

GDPR compliance: where technology is impacted

The need for technology innovation arises across the GDPR. Some requirements that demand technology functionality include:

- *Article 15* – Right of access by the data subject
- *Article 16* – Right to rectification
- *Article 17* – Right to erasure (right to be forgotten)
- *Article 18* – Right to restriction of processing
- *Article 19* – Notification obligation regarding rectification or erasure of personal data or restriction of processing
- *Article 20* – Right to data portability
- *Article 21* – Right to object
- *Article 22* – Automated individual decision-making, including profiling
- *Article 25* – Data protection by design and default
- *Article 35* – Data protection impact assessments

Technology failure and consequences for organisations

Organisations that fail to translate the requirements of the GDPR into their technology run the risk of operational failure, which can, in turn, lead to reputational and legal damage. The key legal consequences will include:

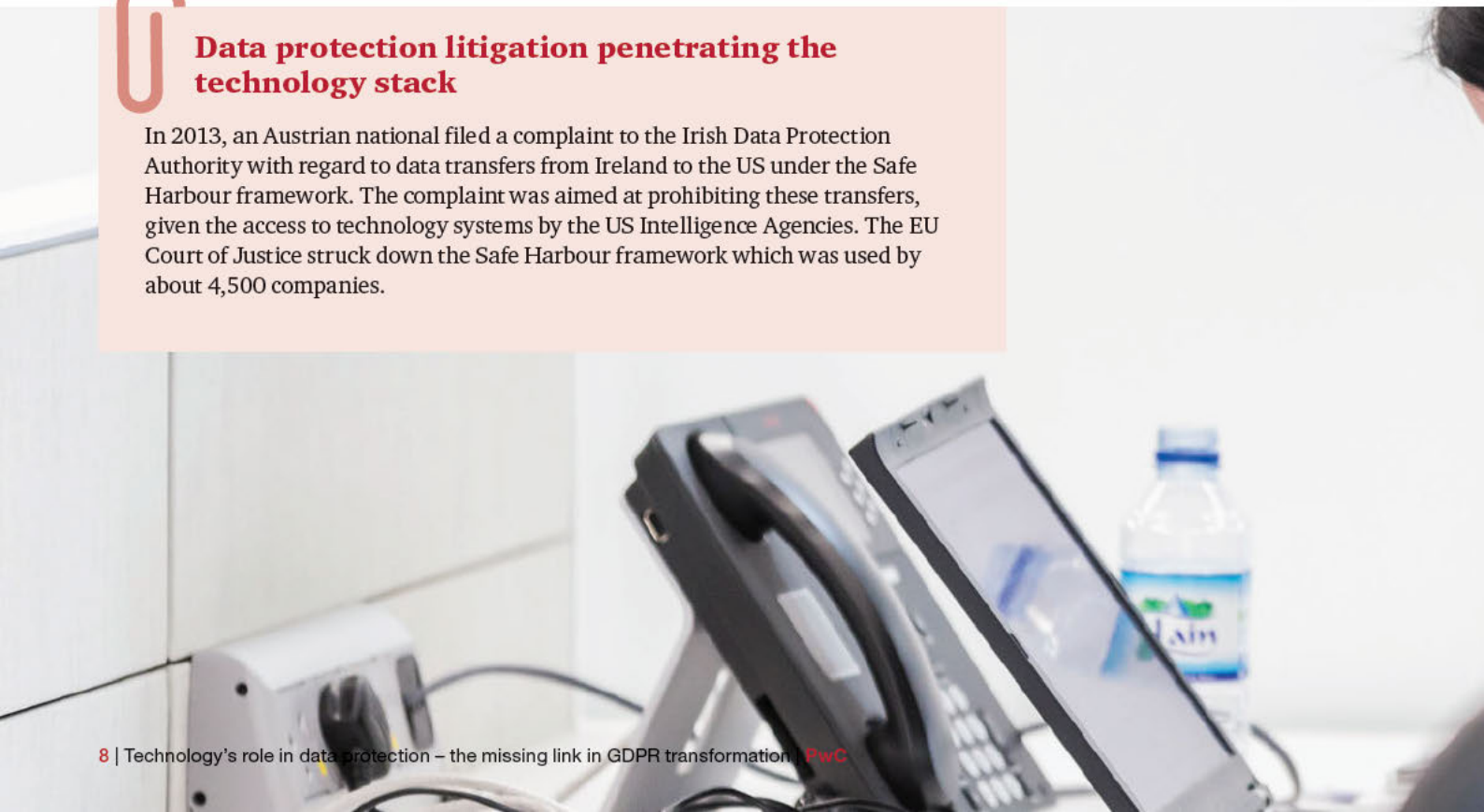
- Regulatory investigations and inquiries, during which the organisation can be required to disclose its records, risk assessments, technology designs, audit reports and other assessments and incident logs.
- Regulatory enforcement orders, which can extend to stopping the use of personal data by an organisation, and the redesign of business processes and the technology environment.
- Regulatory fines, subject to a cap of 4% of annual turnover.
- Exercise and enforcement of individuals' rights.
- Compensation claims by individuals who feel their rights have been impacted.

Examples of operational failure leading to adverse scrutiny of technology

The breach notification rules will of course impact on security and confidentiality problems outside the technology stack, such as employees leaving papers in public places. But most cases will be concerned with technology failure, whether in the sense of external attack (from hackers, malware etc.), poor configuration (e.g. too many people with access rights, or a lack of encryption), or poor operation (e.g. emailing sensitive information to the wrong recipient). When these cases are reported to the regulators and the people affected, they open up lines of inquiry into all aspects of technology design and delivery. A security breach involving the emailing of personal data to the wrong recipient might, for example, develop into a case about data storage and retention.

Data protection litigation penetrating the technology stack

In 2013, an Austrian national filed a complaint to the Irish Data Protection Authority with regard to data transfers from Ireland to the US under the Safe Harbour framework. The complaint was aimed at prohibiting these transfers, given the access to technology systems by the US Intelligence Agencies. The EU Court of Justice struck down the Safe Harbour framework which was used by about 4,500 companies.



Likewise, the exercise of individual rights has the potential to open up the entire technology environment to investigation. If individuals try unsuccessfully to prevent the use of their personal data for marketing purposes, they might take their case to the regulator and trigger lines of inquiry into how all of the individuals' rights are handled by the organisation in question, which can bring technology into focus.

Is the GDPR a bad idea?

The enforcement and litigation risks associated with the GDPR are such that no organisation wants to be exposed to them. However, tough enforcement mechanisms are part and parcel of most important pieces of regulatory law, and it would be a mistake to regard the GDPR as a bad idea just because it exposes organisations to legal risk.

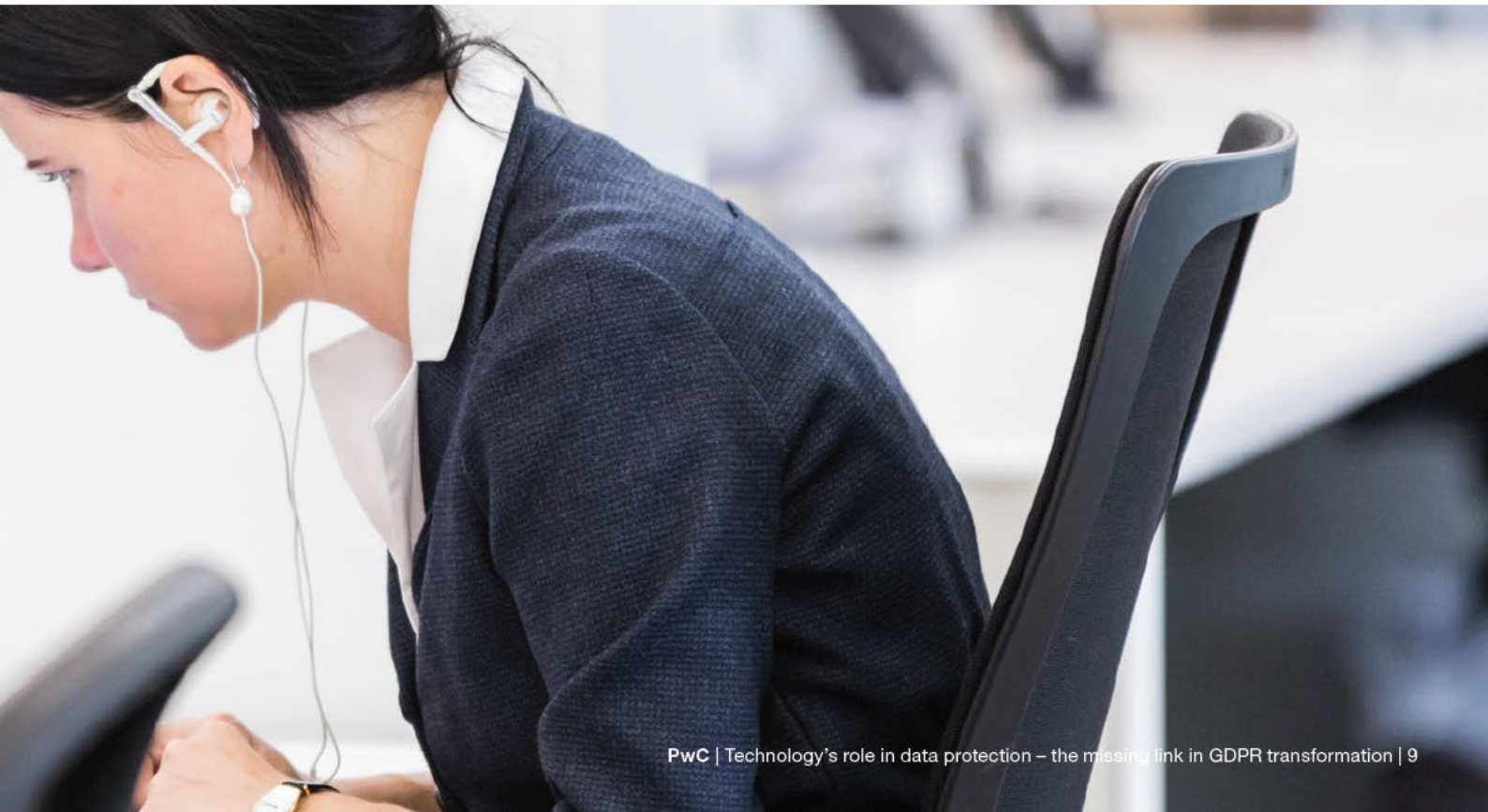
The GDPR can be seen in another light. If questions of legal risk are set aside, what is left is a legislative regime for good data handling. The idea that there should be principles in place for the management of data, that risk assessments should be performed, that controls should be adopted to deliver on the data protection principles and to manage risk, are non-controversial from the perspective of good data handling. Good data handling can also be a driver for other gains, such as competitive advantages in the market, costs savings and wider innovation. Conversely, dealing with failure can generate significant loss and damage.

'Privacy and innovation – not privacy or innovation'

In her first speech as the Information Commissioner of the UK, Elizabeth Denham highlighted a key point for the future of personal data protection: *'It's not privacy or innovation – it's privacy and innovation'.*

Businesses often see compliance as an offset of their time and resources, but the cost of non-compliance will increase significantly. Her advice to businesses is that *'the personal information economy can be perfect for everyone. Get it right, and consumers and business benefit'.*

Elizabeth Denham, Transparency, growth and progressive data protection, 29.09.2016



Technology capabilities required for GDPR compliance scenarios

The role of technology in the GDPR, as both the cause of the problem and as the inevitable solution, leaves organisations in a difficult position. In many organisations, the information management and governance environment is an underdeveloped part of the technology stack. This is because these initiatives regularly lose out to business-sponsored projects with a more direct connection and visible impact on core business metrics, such as revenue, cost and customer satisfaction.

The GDPR poses many operational challenges that are difficult for technology to deal with:

- Technology thrives on certainty, rules and clear requirements, yet the GDPR is both complex and open to interpretation.
- The GDPR requires the enterprise to manage all personal data, yet many organisations do not know where all their personal data resides.
- The GDPR requires the enterprise to control the processing of all personal information, yet the rise of shadow IT takes control away from the IT department and disperses it across the business functions.
- Finding impartial reliable advice is difficult with an explosion of solutions on the market that promise great things but have not had the time to mature and prove their credibility.

The GDPR however now provides the incentive for business to address data privacy through technology and the technologist needs to understand the range of capabilities that can be deployed to achieve compliance.

PwC's framework for evaluating GDPR technology

PwC's GDPR technology framework describes the core technology capabilities and components needed to address the functional requirements of the GDPR. It comprises five domains of Govern, Identify, Act, Analyse and Secure. These are further broken down into 16 technical capabilities or enablers that together would be required to meet the full set of functional requirements demanded by the GDPR across the spectrum of both structured and unstructured personal data. At its most fundamental level, it is describing data management best practice in the context of the GDPR. Adopting such a model should not be viewed as a burden or cost but as a means of extracting the optimal value from what is increasingly seen as one of the most important assets of an organisation – its data.

The GDPR technology framework is intended to cater for all potential GDPR technology requirements, and can be used as a basis for assessing the capabilities of a current technology stack and determining core gaps in basic functionality. In practice, a risk-based approach may de-prioritise certain components if the requirement can realistically be catered for by a combination of manual, policy or procedure remediation strategies.

Govern

Case management

Systems for managing data subject requests, complaints and communications surrounding emergencies including personal data breaches.

Controls management

Systems to manage the control framework for all elements of personal data.

Privacy compliance systems

Systems that manage data protection impact assessments, identify risk gaps, demonstrate compliance and record data purpose.

Training

Robust training solutions or systems that can demonstrate staff GDPR understanding and compliance.

Identify

Data discovery

Systems that analyse both structured and unstructured data across an enterprise to identify personal data.

Data mapping and modelling

Systems that tag all data related to an individual and can demonstrate how all elements link together.

Consent management

Systems that manage, track, and demonstrate all relevant GDPR consent provisions.

Act

Data security

Deployment of systems that protect data through the use of encryption, pseudonymisation and other security technologies.

Data maintenance

Systems to manage data quality, including update and amendment of data throughout the data lifecycle. This must include data deletion and suppression as a key function.

Breach response

The deployment of systems which will in real time detect, manage and resolve breaches (e.g. identify breached data, identify impacted users and notify all relevant parties).

Analyse

Activity monitoring driven by analytics

Analyse how data is being accessed and used, by whom, and how value can be derived from it.

Omni-channel management

Systems to manage and coordinate data coming in from multiple channels.

Archive management

Systems to ensure archive data is managed and deleted in accordance with stated and agreed retention policies.

Secure

Network security

Deployment of comprehensive and integrated network and cyber-security procedures, systems and processes to provide enhanced levels of network security.

Application security

Deployment of systems to ensure all applications that store, process and manage personal data are secure.

IT infrastructure security

Deployment of systems to protect all IT infrastructure, including cloud solutions, used for data management, processing, storage and archiving.

GDPR compliance scenarios

To demonstrate how the technology framework relates to the real world of the GDPR, the following three illustrative scenarios describe the appropriate capabilities required to form an end-to-end solution.

Personal data assessment

To understand what personal data is held and where the data is being stored across the technology stack.

This requires a combination of capabilities across data discovery, data mapping and consent management tools, to identify and manage sources and flows of structured and unstructured personal data across the technology stack and to ensure that consent for specific purposes exists. It also requires data maintenance tools to maintain the accuracy, adequacy and relevancy of personal data and a security system to protect the personal data managed by the organisation. To do this at scale will require automated PII analysis and tagging.

Defensible disposition

To dispose of personal data which is not being stored for a legitimate purpose, is not accurate, has exceeded its retention period, or where consent from the data subject does not exist.

This requires a combination of capabilities across controls management, privacy compliance and consent management to determine the legitimate use of personal data and the internal policies for data management. It also requires capabilities across data discovery and data mapping to identify personal data that breaches the organisation's rules, across data security and data maintenance to rectify, anonymise, delete, pseudonymise, suppress or encrypt the data, and across archive management to ensure personal data is not being retained inadvertently within archives and backups. Maintaining an audit of activity is best practice to support future investigations.

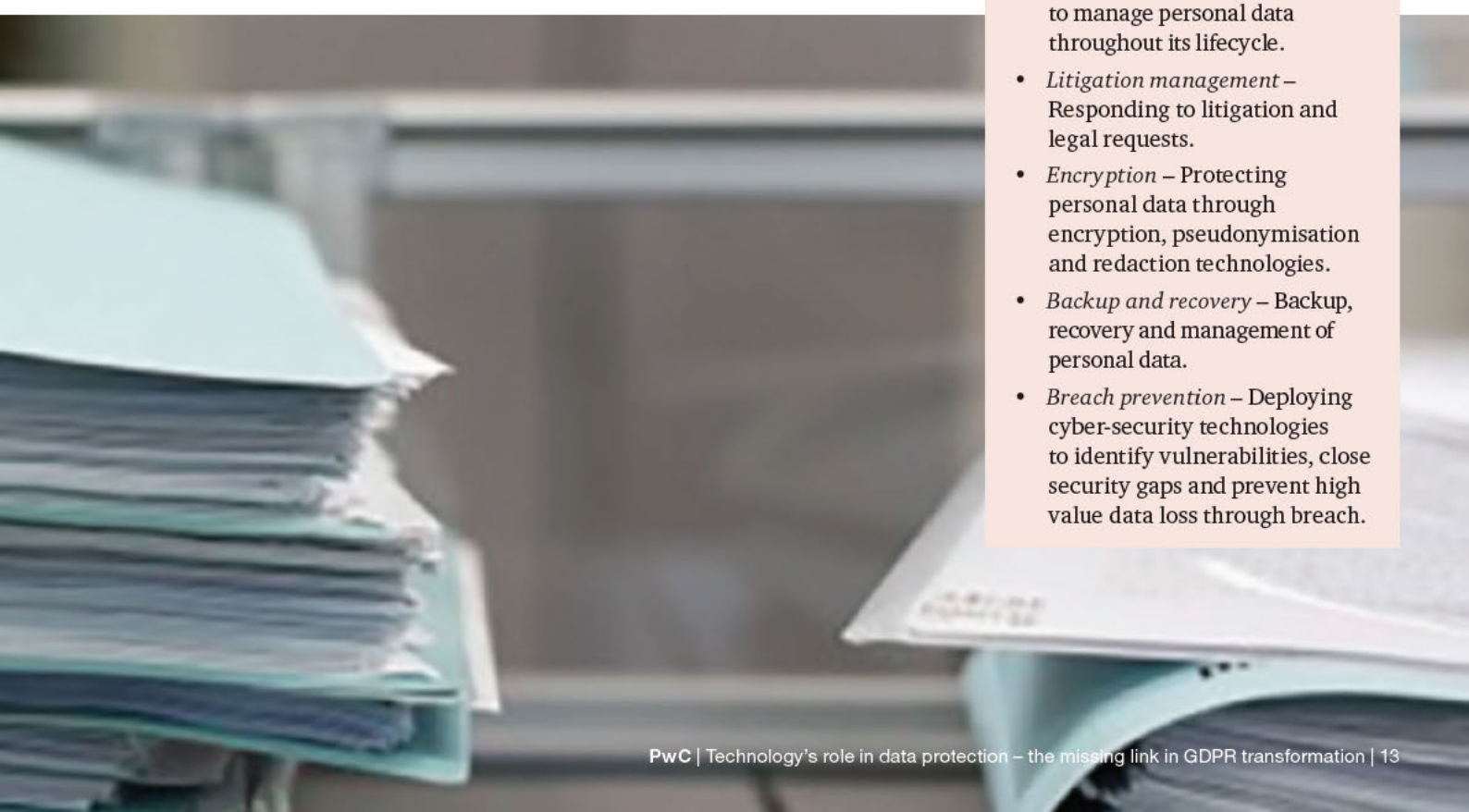
Breach detection, response and reporting

To take all reasonable measures to avoid breach and notify the GDPR supervisory authorities within 72 hours of a personal data breach, take prompt remedial action and notify data subjects without undue delay.

This requires a combination of capabilities across training to provide employees with the understanding and awareness to change behaviours and reduce the risk of security breaches, a robust cyber-security environment to minimise the technical risk of a successful malicious attack on data or application vulnerabilities, and to identify a breach when one has occurred, and a breach response toolkit to manage the response process, including breach investigation, notification and responding to enquiries.

Additional scenarios

- *Policy based governance* – Applying and enforcing policies to manage personal data throughout its lifecycle.
- *Litigation management* – Responding to litigation and legal requests.
- *Encryption* – Protecting personal data through encryption, pseudonymisation and redaction technologies.
- *Backup and recovery* – Backup, recovery and management of personal data.
- *Breach prevention* – Deploying cyber-security technologies to identify vulnerabilities, close security gaps and prevent high value data loss through breach.



Moving from theory to reality – understanding and utilising the consensus of professional opinion

No legislative text can provide exhaustive instructions on how to deal with every permutation of the issues that may arise in its area, and in this sense the GDPR is no different, despite containing a built-in 'user manual' for change. There is considerable 'white space' that still needs to be filled.

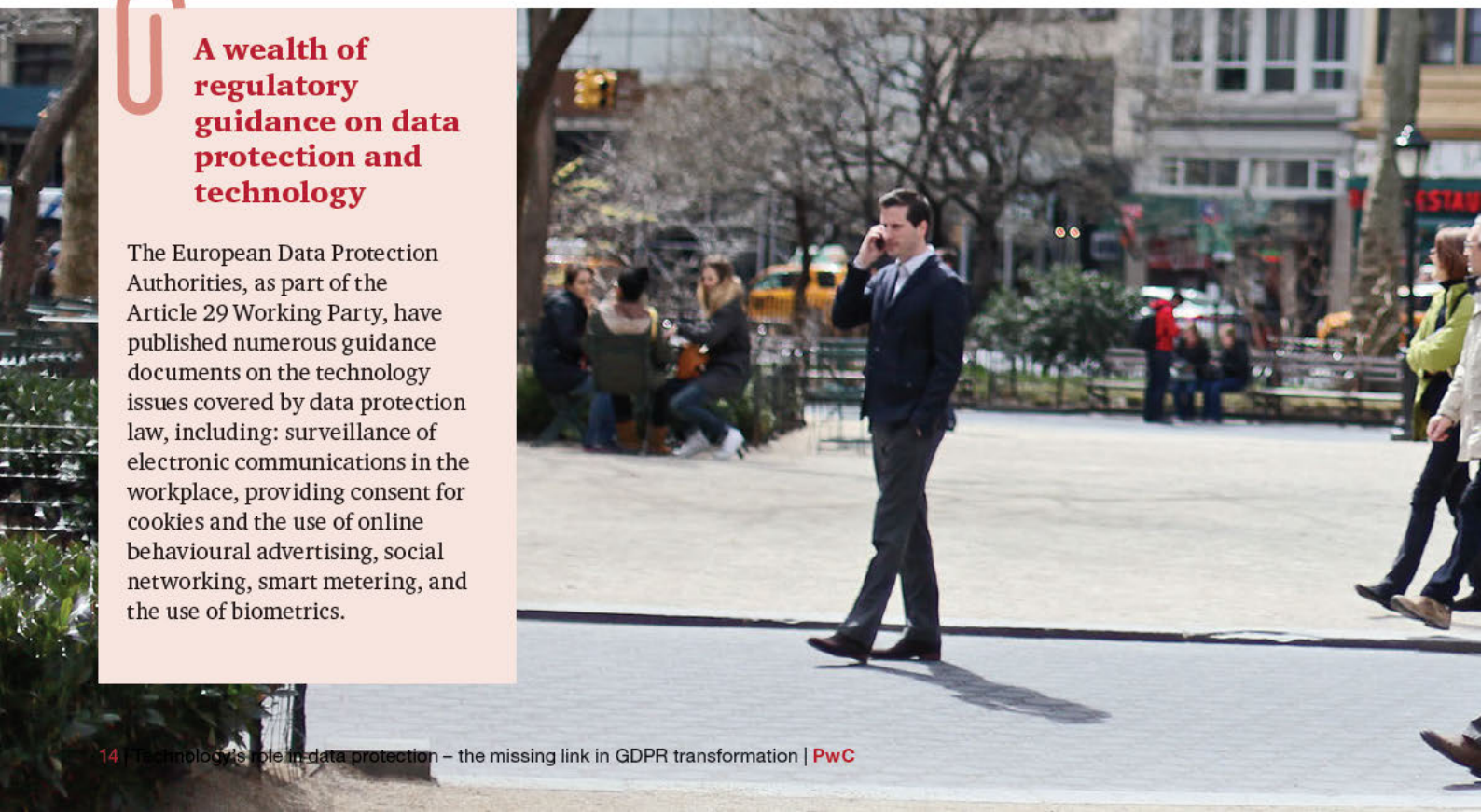
Regulatory guidance on technology issues

The regulatory system provides considerable assistance on the detailed requirements of the law. Organisations that have been tracking developments in regulatory guidance for technology will be very much aware of the Article 29 Working Party, which brings together the EU Data Protection Authorities and representatives of EU Institutions, to develop guidance on discrete points of concern in the law.

This guidance shows that regulators are up-to-date with technology issues. The regulators will expect organisations to be familiar with the Article 29 Working Party's guidance. It is required reading.

A wealth of regulatory guidance on data protection and technology

The European Data Protection Authorities, as part of the Article 29 Working Party, have published numerous guidance documents on the technology issues covered by data protection law, including: surveillance of electronic communications in the workplace, providing consent for cookies and the use of online behavioural advertising, social networking, smart metering, and the use of biometrics.



The technology landscape – working with technology experts

Delivering the data protection principles and individuals rights in technology also needs a strong awareness of the range and nature of the technology options available in the market.

This points the GDPR programme owner in four directions: the expert functions in their organisations that are responsible for the technology environment (CIO, CTO, CISO etc.), technology professional services providers, technology analysts, and technology vendors. Regulators will expect organisations to have a process in place that takes account of the need for expert advice and support.

Regardless of the domain of expertise relied on, organisations will need to be confident that their experts are intimately familiar with the requirements of the GDPR. A technology vendor should map its products and services to the requirements of the GDPR in order to understand the extent to which they can usefully support a GDPR programme in a granular sense. For example, two primary roles that technology can play within a GDPR programme are (1) classifying information that is within the scope of the GDPR, and (2) applying appropriate policies to that information (e.g., move, delete, quarantine, redact, notify, encrypt) – technology vendors should be able to describe where they fit into these roles. Other characteristics to look for include GDPR track record, market reputation and the ability to provide strategic support so that the technology design is future-proofed.

What should organisations do now?

It will already be clear that many organisations will need to elevate the importance of technology within their GDPR programmes. Technology needs to be brought into planning and decision-making processes early on within change programmes – it must be one of the key considerations for an organisation in making decisions about meeting its requirements and mitigating the risks.

Organisations should reflect on the fact that technology projects are lengthy exercises, and even a straightforward data management initiative with a singular objective in a well-run, well-resourced organisation can take 3 to 6 months to complete. When the clock is ticking fast, a 'wait and see' attitude is not an option. Action directed by a Vision and Strategy needs to be taken now. Indeed, when considering an approach to the challenges of the GDPR, we see too many enterprises rushed into undertaking 'purposeless activity' or 'activity for activity sake'. Setting the Vision and Strategy for the GDPR based on a mature assessment of an organisation's economic goals for personal data, its risk positions and its full range of obligations, is the first task. From that foundation, there are four key activities that organisations should initiate:

1. Call to action to engage a diverse and senior stakeholder group to drive GDPR change.
2. Assess the gap between functional GDPR requirements and technology capabilities.
3. Prioritise and sequence the change required by executing a risk and cost/benefit analysis.
4. Design and mobilise the GDPR transformation programme for change.

Call to action to engage a diverse and executive stakeholder group to drive GDPR change

Organisations seeking to achieve GDPR compliance will need to engage multiple stakeholders across a range of functions (IT, Compliance, Legal, HR, Customer Service, Marketing, etc.) to gather the organisational backing for the changes required. In building this coalition, it is important to note that, as well as achieving GDPR compliance, the consequent improvements of adopting good data management and security principles can deliver tangible benefits back to the enterprise. These include:

- Driving commercial performance through higher quality and more accurate data.
- Greater insight into customer needs leading to improved customer satisfaction.
- Considerable cost reduction opportunities by reducing IT infrastructure footprint.
- Opportunity to simplify the applications landscape.

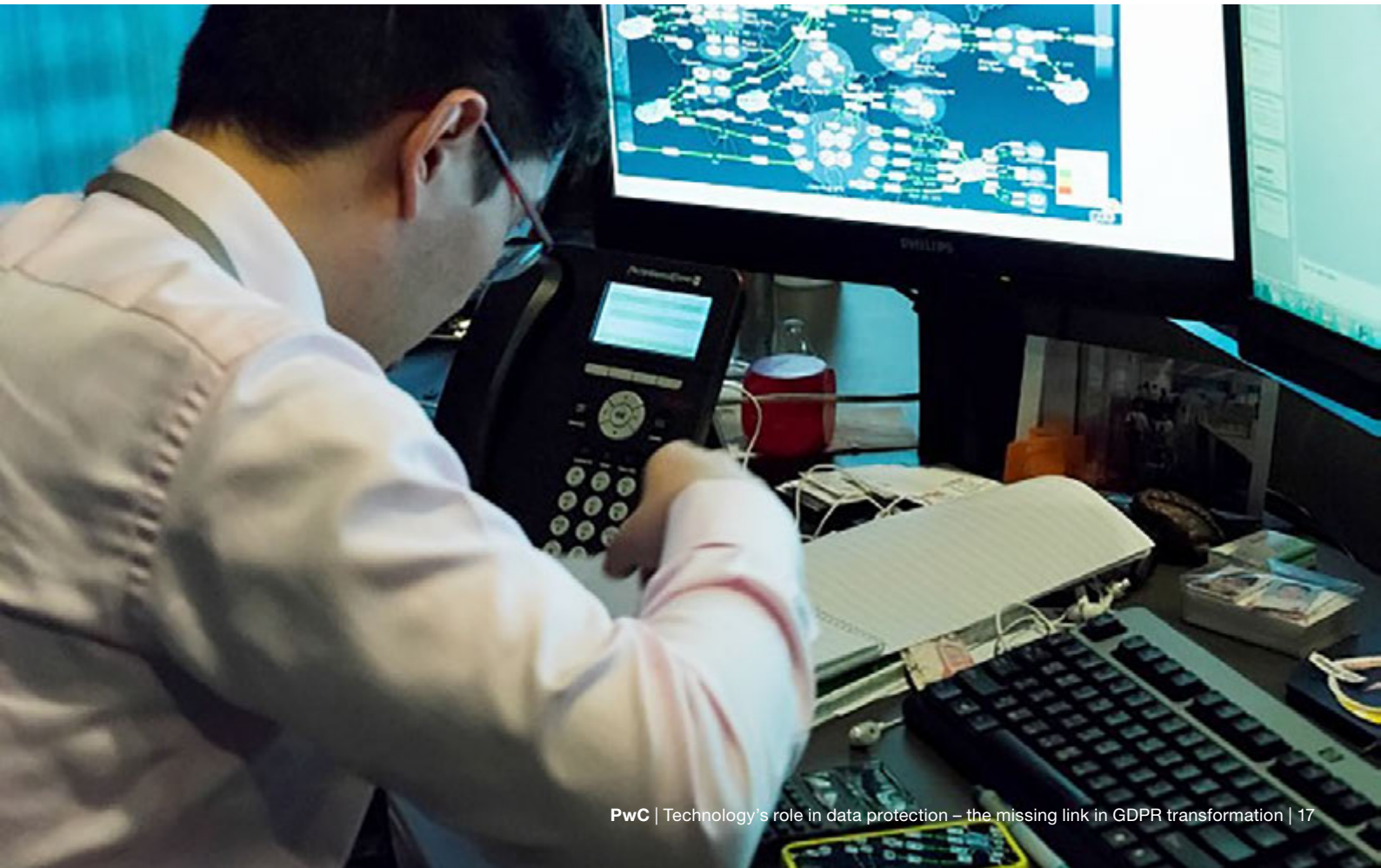
The stakeholder group will be instrumental in securing budgets, resources, generating urgency and clearing the path for a consolidated programme with the backing of the board and executive.

Assess the gap between functional GDPR requirements and technical capabilities

Enterprises should undertake a technology functionality gap analysis, whereby the technology-driven requirements of the GDPR are assessed against the technology capabilities of the organisation, covering the entire data lifecycle management process and its associated policies, infrastructure, security and controls. The requirements will be driven by the Principles, Rights and Build requirements of the GDPR and the gap analysis will expose deficiencies, vulnerabilities, potential threats, and areas of non-compliance.

Prioritise and sequence the change required by executing a risk and cost/ benefit analysis

In the world of technology just about anything and everything is possible. It's simply a question of having enough time and money. In the real world however, both are limited resources, and is why we view the only realistic way to address the GDPR's requirements is through a risk-based approach, where the highest risk areas are addressed first and most comprehensively. Accordingly, enterprises should use the findings of their gap analysis, a cost/benefit analysis and scenario testing to identify and plan their priorities.



Design and mobilise the GDPR transformation programme for change

A GDPR programme will be complex and transformational in nature, as it will change the way the organisation's people, processes and technology interact around the handling of personal data. Simply treating the change as a project is likely to end in failure. Instead, an integrated transformation programme structure should be adopted. Aspects of this programme approach will involve:

- Operating model for GDPR with associated organisation change.
- Compliance implementation of policy, procedure and control design and implementation.
- Operational change and process redesign.
- Technology programme consisting of detailed design, build, test and deployment.
- Management of change activities including communications, training and behaviour change.
- Programme and project management to govern the programme.

As well as deploying expertise from within an enterprise, a programme of this nature will most likely also require the involvement of external SMEs and technology vendors to provide specialist knowledge and experience.

The role of advisors and vendors

While the GDPR technology framework is intended to provide a comprehensive view, organisations will have to make difficult choices about when, where and what to invest in to provide maximum protection. While some will have the scale and resources to deploy technology covering the entire GDPR technology framework, most will assess risks differently and deploy resources in a more focused manner.

The expertise to advise on and deploy technologies will often not exist within an organisation. Professional advisors, software vendors, IT service companies and the contractor market are resources which can plug capability and capacity gaps, especially where they bring proven expertise and understanding about the specific challenges of the GDPR.

Selecting software with tailored functionality to address the different needs of the GDPR is one means of addressing a capability gap. But with so many new GDPR solutions in the market, selecting a vendor can sometimes feel like a shot in the dark. As with any software selection, addressing this question on the basis of strategic fit to long-term strategic needs, as opposed to addressing an immediate issue with a tactical solution, is a key starting point. Additional factors for vendor selection of GDPR solutions may include:

- Breadth of an integrated portfolio and interoperability with other vendors' solutions.
- Depth of analytics embedded into the solution to drive effectiveness and efficiency.
- Proven data privacy, data security and sector domain experience.
- Simplicity in packaging, such as a modular approach to procuring and deploying solutions.
- Market reputation, longevity and roadmap for product development around the GDPR solution set.

The complexity of a GDPR programme is significant and the time to act is now. That means building the right team to deliver GDPR compliance is critical. Careful consideration should be given to selecting the right partners to assist an organisation in achieving the strategic imperative of GDPR compliance.

[1] Council of Europe Recommendation 509 on human rights and modern scientific and technological developments, 31 January 1968

[2] For example, see the Information Commissioner's guidance on CCTV, 'Business could face fines for ignoring CCTV data protection law', 2 February 2017. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/02/businesses-could-face-fines-for-ignoring-cctv-data-protection-law/

[3] By 2019 47% of all technology spend is expected to be funded directly by non-IT functional units – IDC IT Spending Guide – https://www.idc.com/getdoc.jsp?containerId=prUS41026616

About the authors

Stewart Room
Partner, PwC UK
Joint Global Head of Data Protection;
Global Cyber Security and Data Protection Leader;
UK Data Protection Leader

M: +44 (0)7711 588978
E: stewart.room@pwc.com

Peter Almond
Director, PwC UK

M: +44 (0)7793 758029
E: peter.almond@pwc.com

Kayleigh Clark
Senior Associate, PwC UK

M: +44 (0)7841 468403
E: clark.kayleigh@pwc.com

171201-151555-WB-OS