Deloitte.

May 2016

Governance *in brief*
EU Privacy Legislation

Headlines

- Privacy and Data Protection issues present a growing challenge, requiring organisations to interpret and comply with complex and diverse international laws and regulations on how they handle personal data.
- These challenges are set to increase dramatically with the introduction of the European General Data Protection Regulation (GDPR), which will be enforced from mid-2018.
- More and more organisations are recognising that the responsible use of people's data allows privacy to be a business enabler rather than just another compliance headache. Getting privacy right means capturing the trust and confidence of consumers who are in turn more likely to repay you with loyalty and access to much sought after personal data.

Background

Within the EU, the European Data Protection Directive 95/46/EC (DP Directive) currently regulates how personal data can be processed. The DP Directive is based around eight core principles covering the security, accuracy, storage, retention and destruction of personal data as well as notifying users of the use of their data, restrictions on direct marketing and requirements concerning international transfers.

These rules have recently changed with the introduction of the GDPR, which features enhanced restrictions on the processing of personal data, and increased fines for non-compliance. There has never been a more important time for organisations to get privacy right.

What is Privacy?

Privacy refers to the right of individuals to have a certain degree of control over the collection of their personal data, the ways in which this data is used, who it is shared with, and how long it is retained. Within Europe, this right is enshrined within Article 8 of the European Convention on Human Rights, which explicitly provides a right to respect for each individual's 'private and family life, his home and his correspondence'.

Personal data is defined as information relating to an identified or identifiable living individual. This includes information that can be used either directly, or in combination with other information, to identify the individual. Examples of personal data include name, email address, telephone number, IP address and any other 'unique' identifier.

Processing is defined very broadly, encompassing any operation or action carried out on information or data. Activities such as obtaining, recording, holding, sharing or deleting information or data will all be regarded as processing activities.

Why does privacy matter to your business?

There are three key drivers that are making organisations more sensitive to privacy issues than ever before:

- **Legislative challenge**: The rules governing the processing of personal data are complex, ever changing and vary across the globe. European Data Protection law has recently been overhauled, with the introduction of additional administrative burdens and new requirements on organisations.
- **With big data comes responsibility**: The opportunity to profit from customer data needs to be counter-balanced with legal and ethical considerations. By using personal data in a responsible, controlled and transparent way, organisations are able to develop a trusted relationship with their customers.
- **Reputation protection**: Maintaining a consistent approach to privacy compliance and data governance, whilst operating across multiple jurisdictions, brands and channels presents a challenge to many organisations. Failure to do so can result in significant attention from both consumers and regulators – attention of the wrong sort.

EU General Data Protection Regulation

Over the past four years the European Commission has focused on overhauling EU Data Protection legislation, culminating in the introduction of the new General Data Protection Regulation (GDPR). The GDPR introduces regulatory requirements that will impact organisations across all sectors. These requirements concentrate on improving consumer protection and harmonising existing EU privacy laws, but also introduce extra burdens and restrictions for organisations that collect, store or use personal data relating to EU citizens.

With the rules set to be enforced from 25 May 2018, organisations are likely to face a variety of new technical and procedural challenges. Failing to act promptly could lead to difficulties in aligning or updating policies and procedures to meet the new requirements in time. This could result in fines for non-compliance, reputational damage or missed opportunities to demonstrate to customers that their data is treated responsibly.

Timing

On 14 April 2016, the EU Parliament approved the final text of the GDPR, which was published in the Official Journal of the European Union on 4 May 2016. Organisations will be given a grace period of two years in which to achieve compliance with the requirements. The new requirements will start to be enforced from 25 May 2018.

Key impact and requirements

Privacy as a concept is broad and far-reaching. For this reason the GDPR impacts many areas of an organisation, and it can't be treated as simply a legal issue. Key areas likely to be impacted are summarised below, along with Deloitte's perspectives on the new regulation.

Record keeping, compliance and potential fines:

The GPDR introduces an enhanced set of requirements and challenges for legal and compliance functions to manage, including:

- **Enhanced enforcement**: Gross non-compliance could result in fines of up to 4% of annual global turnover. The regulatory reach extends to organisations outside the EU that process EU citizen data, even if they have no legal presence in the EU.
- **Accountability**: In lieu of the requirement to make annual processing notifications, the GDPR introduces significant new requirements around maintenance of audit trails and data journeys. This is most likely to impact consent management; if a consumer challenges the accuracy of given consent, it is now the business that bears the burden of proof.
- **Data Protection Officers**: Those organisations processing personal data on a large scale will now be required to appoint an independent, adequately qualified Data Protection Officer. This will present a challenge for many medium to large organisations, as individuals with sought-after skills and experience are currently in short supply.
- **Privacy Notices and Consent**: Organisations will now have to invest heavily in way they construct their public-facing privacy policies. It will no longer be good enough to hide behind pages of legalese, but at the same time the information that has to be provided has increased. Could this mark a turning point in the way organisations approach this aspect of privacy? Could we see Communication teams drafting policy copy instead of lawyers?

Technology:

Organisations' use of technology to enable information security and other compliance initiatives will need to be reconsidered, in line with new requirements introduced by the GDPR.

- **Privacy-by-Design and by default**: Organisations will need to change the way they design, build, and deploy technology, to ensure that privacy controls are built into them. IT governance frameworks will need to be reviewed and updated to meet these requirements.
- **Online**: Strict new requirements on online profiling and tracking are being introduced, significantly impacting direct to consumer businesses, including a requirement that this activity only be carried out where consumers have provided their consent. Where data processing activities across digital assets are highly complex, from mobile apps to wearable devices, this is likely to present a significant challenge.
- **Incident Management**: The GDPR will require systems to be tested to protect against incidents. Significant breaches will have to be reported to regulators and in certain cases also to consumers, requiring organisations to revise their incident management procedures and retain a sufficiently detailed log of breaches.
- **Encryption**: The GDPR formally recognises the privacy benefits of tools such as encryption. Data Loss Prevention and Identity and Access Management solutions will also become increasingly important under the GDPR.

Data:

Information management requirements have always supported privacy initiatives, but the GDPR requires activities which specifically link to compliance demands.

- **Data Inventories**: Organisations will have to take proactive steps to demonstrate they know what data they hold, where it is stored, and who it is shared with, by creating and maintaining an inventory of data processing activities. Data leads will have to work closely with privacy colleagues to ensure this work is carried out and covers all necessary bases.
- **Right to Data Portability**: A new right to 'data portability' means that individuals are entitled to request copies of their data in a readable and standardised format. The challenges for this requirement are numerous: achieving clarity on which data needs to be provided, extracting the data efficiently and providing data in an industry-standardised form are the main hurdles.
- **Right to be Forgotten**: An even stronger 'right to be forgotten' is further evidence of the consumer being in the driving seat when it comes to use of their data. How will this work in practice? Arguably the most difficult of all the new requirements to implement correctly, the right to be forgotten could require wholesale reviews of processes, system architecture and third party data access controls.
- **New Definitions of Data**: The GDPR recognises the concept of pseudonymous data – data that does not allow an individual to be identified without additional information. It also expands the definition of personal data, placing a greater emphasis on data classification and governance within an organisation.

Recommendations for advance preparation

Examples of some initial key steps that should be taken to help prepare for, and assess the effort required to comply with, the GDPR are provided below:

- Perform readiness assessments across key areas of the business, to gauge how current practices match up to the requirements of the GDPR and start to develop a compliance roadmap.
- Identify the location of your main establishment, to confirm which Data Protection Authority will act as lead supervisor.
- Raise awareness of the forthcoming changes under the GDPR amongst key stakeholders and decision makers – this should include education sessions for the board.
- Review privacy governance structures and operating models, verifying that accountability for privacy is appropriately assigned and that Data Protection Officers are designated, where required.
- Establish procedures to create and maintain internal inventories of IT systems, websites, mobile applications and other repositories of personal information.
- Review privacy risk management procedures, building privacy impact assessments into wider project management methodologies.
- Update incident management procedures to address breach notification requirements.
- Expand and rewrite privacy notices to reflect enhanced transparency requirements.
- Review the limitations of relevant IT systems and technology, with respect to processing data portability and erasure requests.

'Safe Harbor'

In October 2015, The Court of Justice of the European Union ruled the EU-US 'Safe Harbor' framework for transferring personal data from the European Economic Area to the US invalid. The extent of this ruling was far reaching, impacting thousands of companies who have self-certified using the Safe Harbor framework and thousands more who relied on the framework to legitimise transfers of personal data to the US.

Following the ruling, businesses, regulators and European policy makers worked hard to reinstate legal certainty for businesses and safeguard the transatlantic flow of data – critical for the European economy. In February 2016 a new legal framework for such transfers was agreed, the EU-US 'Privacy Shield'.

The EU Commission has confirmed that this updated framework will strengthen previous requirements under Safe Harbor, through the introduction of:

- Strong obligations on companies handling Europeans' personal data and robust enforcement
- Clear safeguards and transparency obligations on U.S. government access
- Effective protection of EU citizens' rights with several redress possibilities

Whilst preliminary agreements have been made, a final decision is still pending concerning the adequacy of the Privacy Shield framework to meet EU privacy legislation.

Further information:

The final text of the General Data Protection Regulation can be found at **http://eur-lex.europa.eu**

Deloitte View

The new requirements introduced by the GDPR are likely to require major changes in the way organisations collect, use, handle and store personal data. The threat of increased monetary penalties, combined with increasing demands from consumers, has already caused privacy to shoot to the top of the boardroom agenda for many organisations.

While regulators will give a 2 year 'grace' period to achieve compliance, it will be vital to consider the impact that these changes will have, and to plan now for the required improvements and changes to existing policies, procedures and practices.

Contacts – Data Privacy Practice

Our experienced team of privacy professionals can deliver a wide range of services, from quick-win readiness assessments to full privacy remediation programmes. Our European data privacy practice has a reputation for tackling complex issues, working across industries and jurisdictions to translate complex regulatory requirements into scalable, practical programmes. Our team have extensive experience in operationalising privacy; creating business-focussed solutions to privacy compliance requirements and establishing sustainable, long-term change within organisations.

Based in the Deloitte Technology Consulting practice, our privacy team works closely with technology and data experts, which allows us to offer a holistic view of legal and compliance, technology, and data. Contact a member of the team for further information. To speak to a member of our team, please contact **Peter Gooch**, our UK Privacy Practice Lead.

Peter Gooch – 020 7303 0972 or **pgooch@deloitte.co.uk**

Richie Evans – 020 7007 6734 or **richievans@deloitte.co.uk**

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through a series of briefings and bespoke training. Membership of the Deloitte Academy is free to board directors of listed companies, and includes access to the Deloitte Academy business centre between Covent Garden and the City.

Members receive copies of our regular publications on Corporate Governance and a newsletter. There is also a dedicated members' website **www.deloitteacademy.co.uk** which members can use to register for briefings and access additional relevant resources.

For further details about the Deloitte Academy, including membership, please email **enquiries@deloitteacademy.co.uk**

Contacts – Centre for Corporate Governance

Tracy Gordon – 020 7007 3812 or **trgordon@deloitte.co.uk**

William Touche – 020 7007 3352 or **wtouche@deloitte.co.uk**

Corinne Sheriff – 020 7007 8368 or **csheriff@deloitte.co.uk**

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. J6483