GDPR journey: from ready to compliant
GDPR survey results
Readiness at a glance

The General Data Protection Regulation (or ‘GDPR’) took full effect on 25 May 2018. As a key data protection regulation, the GDPR has changed the way organisations treat personal data. The regulation has introduced many changes to data protection, including broadening territorial applicability and scope, enhancing and extending the data protection principles, shortening timelines, and making data processors accountable along with data controllers for the personal data processing. Previously, Deloitte Ireland published a number of articles about the GDPR and its impact on the organisation, which can be found on our website.1

Deloitte Ireland carried out a survey to gain an understanding on how Irish organisations are tackling the challenges that the GDPR imposes. At a glance, the survey revealed that organisations addressed a number of the GDPR requirements, and reached a defensible position. However, GDPR compliance is not a once off project. Instead, it is wide range of activities required to ensure continuous management of the risk going forward.

Furthermore, the principle of accountability requires organisations to be able to show compliance with the data protection principles. Accountability obligations are ongoing and are not a ‘tick the box’ exercise, but instead, require organisations to be proactive for the personal data that they process in order to demonstrate their compliance with the regulation.

This article outlines an overview of challenges that Irish organisations faced and how they stand now that the regulation is live.

High Level Overview of Preparation
Activities

Compliance with the GDPR required significant effort in addition to specific knowledge and expertise. The challenges that the regulation presented were significant for organisations. Not all organisations had a capacity to have a full-time team dedicated to implement solutions to comply with GDPR into their environment. Therefore, it was not surprising to learn that only 14% of organisations noted that they were ready for the regulation and deemed themselves as fully compliant. The remaining participants indicated being partially compliant.

In the effort to comply with the regulation, organisations carried out the following activities:
- Completed GDPR readiness assessment – 72%
- Appointed a Data Protection Officer (DPO) – 39%
- Added DPO responsibilities to an existing role – 25%
- Fully updated privacy framework – 18%
- Partially updated privacy framework – 57%
- Used existing systems to keep a consent record – 57%
- New systems were introduced to record data subject consent – 18%
- Documented Data Protection Impact Assessment process – 32%
- Used existing data processors due diligence procedures and incorporated new requirements – 39%
- Investigated key IT systems to ensure they can carry out data subject access requests - 39%
- Put data breach management procedure in place - 64%

Possibly the most impactful drivers to comply with the regulation were the changes in the administrative fines for non-compliance or violation. The fines are defined as the following:
- The lessor threshold is a potential fine of €10 million or 2% of total worldwide annual turnover (whichever is greater) for serious breaches; and
- The higher threshold is a potential fine of €20 million or 4% of total worldwide annual turnover (whichever is greater) for very serious breaches.

Therefore, it was not surprising to learn that for more than 50% of respondents high fines acted as an effective motivator to start paying attention to data protection and privacy. What was surprising, however, is that 43% of the companies noted that their leadership already had privacy on their agenda.

To date organisations invested a substantial amount of resources in order to reach a certain level of compliance at the end of May 2018. However, it is important to carry on with the work they started during the preparation for the GDPR. The work will be ongoing and will remain so due to the ongoing requirements, complexities and challenges that organisations face.

Key challenges

Compliance with the GDPR was a challenge and continues to be a challenge for many organisations. During the preparation for the regulation, organisations had difficulty interpreting the requirements and adapting them to their processing environments. For other companies, the timeframe of two years which was given to implement the regulation was a challenge. While organisations found various aspects and elements of the GDPR more or less challenging, the areas that are listed in this section were indicated by the survey respondents as the most demanding and challenging.

Data subject rights
The rights of data subjects under the GDPR are now strengthened and broadened, giving more control to individuals. In addition to existing rights for data rectification and personal data access, now data subjects have right to erasure (“right to be forgotten”), restriction of processing, data portability, and right to object to processing.

More than a third of the organisations indicated that these were the most challenging requirements for them to meet. However, only 14% of organisations indicated that they updated and documented their internal processes to manage data subject requests, and 46% noted that they partially completed this exercise.

Insight
With stricter timelines allowed to fulfil data subject rights, data controllers have to ensure that they have efficient and effective processes and procedures in place to manage data subject rights requests. One of the key elements required to achieve this is the need for organisations to understand their personal data landscape. Personal data can be stored in a number of formats on various storage media (e.g. USB flash drive, mobile phone, CD/DVD, internal, shared or external hard drives etc.). In addition, it is important that organisations understand whether their systems have the capacity to update, restrict processing, extract, delete, pseudonymise or anonymise personal data.

It is a time and resource heavy task. Therefore, it is crucial that the identification of the personal data is not fast tracked, but instead treated as a key activity required to guarantee effective management of data subject rights.

As the regulation does not allow much time to process data subject rights requests, it is critical that organisations implement robust procedures to manage data subject rights.

In addition to having robust processes and procedures in place it is important that organisations understand their IT systems and whether these systems are capable of supporting the management of data subject requests. It is interesting to note that 14% reviewed all IT systems in their organisation, and 39% of organisations investigated their key IT systems. Only 10% of respondents indicated that they did not plan to investigate their IT systems.
Lawful basis and Consent

The GDPR requires that organisations process personal data in line with the lawful bases set out by the regulation. In order to comply with this requirement, it is key that organisations understand and document what lawful basis apply to the processing activities they have, and 43% of the survey respondents noted that they completed this for all personal data processed within their organisation. For other companies this was still in progress.

Consent is one of the lawful bases for processing personal data, and is now subject to additional requirements under GDPR. All consent must be freely given, specific, informed, unambiguous and in some cases explicit.

In order to be compliant with GDPR, organisations had to carry out a full review of their consent mechanisms. They also had to review and update their privacy statements to reflect any changes introduced to their processing environments and align them in line with the GDPR requirements.

For many companies the challenge was to identify whether their current personal data records are based on an appropriate consent, and whether they could demonstrate compliance with the new consent requirements. This has led many companies to a hard decision of whether to cease processing, perform a re-consent exercise, or delete records where consent could not be obtained in line with the GDPR.

As part of the GDPR accountability principle companies have to be able to demonstrate compliance with the regulation. As such, organisations have to show evidence that they collected consent in a lawful manner. There are many ways of doing this, which was noted by the survey respondents. The majority of organisations leveraged the functionality of existing systems to record consent there. Other respondents noted that they plan to implement a new CRM solution (18%), while others were tracking consent manually.

Insight

Understanding and correctly identifying the lawful basis that applies to the processing of personal data is key. Many organisations have historical data that was collected “just-in-case” or for future use. Storing data in legacy systems for these purposes without appropriate ground for it violates the GDPR core principle of lawful, transparent and fair processing.

Therefore, it is crucial that organisations identify and analyse the lawful basis that apply to the personal data that they process. Once embarked on the discovery exercise, it is important that organisations retain the record of the identified personal data, including purposes for processing and an applicable lawful basis.

Where the relevant lawful basis is consent, organisations must ensure that consent mechanisms comply with the higher standard, and appropriate audit trail is maintained to demonstrate compliance.

Where organisations rely on legitimate interest as the lawful basis to process personal data, they have to ensure to justify this decision by completing a Legitimate Interests Assessment, or ‘LIA’. It is important to retain an audit trail of the completed LIA. When changes are made in the processing of the personal data, organisations have to challenge themselves on whether legitimate interest remains the most relevant lawful basis for the processing, and ensure that any changes regarding the processing are reflected in the documented LIA.
Privacy policy framework and Accountability

The GDPR requires that organisations demonstrate compliance with the regulation and take accountability for the processing of their personal data. For organisations to be able to demonstrate how they implemented and aligned their processes to the GDPR, a privacy policy framework with adequate monitoring and reporting lines should be developed in line with GDPR requirements.

Less than 20% of organisations indicated they updated their data protection policies. The remaining majority of organisations noted they are still at varying stages of the review process. Considering that a policy framework is one of the main governing tools that organisations can use to demonstrate their approach to data protection, it was surprising to note such a high number of respondents that did not have a privacy policy framework in place by 25 May 2018.

Data Breach

Data breach notification is a new requirement that the GDPR is enforcing. In addition to the notification requirement, the GDPR poses strict notification timelines of 72 hours for any data breach or potential data breach which is likely to result in a risk to an individual’s rights and freedoms. The regulation also makes it mandatory for the data controllers to notify individuals without undue delay if the breach is likely to result in a high risk to their privacy rights.

In order to adhere to these strict notification timelines, organisations must have efficient data breach identification and reporting structures in place. The result of the survey showed that 61% of the respondents were able to comply with the 72 hour notification requirements. However, one fifth of the respondents did not fully align their processes to the new requirements.

It is interesting to note that there is no notable correlation between the organisations’ sector or size to indicate their ability to meet the challenges of data breach reporting and notification requirements.

Insight

The GDPR explicitly requires that organisations are accountable for the way in which they process personal data and that they are able to demonstrate compliance with the data protection principles. A policy framework is a key tool to ensure that organisations have a defined set of rules on how they address the data protection principles and comply with the Regulation. It is important, therefore, for any organisations that process personal data to implement a data protection policy suite that outlines their commitment to data protection across the organisation.

The data protection suite can vary depending on complexity of the personal data processes and a structure of an organisation. It is key to understand your organisation, culture and processing environment first and foremost in order to identify the best approach for implementing the privacy policy framework.

Insight

Any organisations, big or small, can have a data breach that poses a significant impact on individuals’ rights and freedoms. Therefore, it is crucial to ensure that organisations implement robust data breach identification and reporting processes to ensure that they are reported within the required timelines. It is also important to regularly train staff and inform data processors on the importance of timely reporting of data breaches.

It is invaluable for organisations to incorporate data breach testing into their business continuity and disaster recovery plans, and regularly test various data breach scenarios to gain comfort around the effectiveness of data breach notification procedures in place.
Data Protection Officer
Under Article 37(1) of the GDPR certain organisations are required to nominate a Data Protection Officer (“DPO”). In particular, a DPO has to be designated when:

• the processing is carried out by a public authority or body except for courts acting in their judicial capacity;
• the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
• the core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Based on the survey, 39% of the respondents indicated that they appointed a DPO in their organisation. It is worth noting here that 27% of these organisations are in the manufacturing sector, a sector that is often not perceived as data controllers that processes large amount of personal data as part of their core activity. Only 7% of respondents indicated that they did not plan to appoint a DPO.

The Article 29 Working Party issued additional guidance on the role of a DPO, which notes that the DPO can be sourced internally if there is no conflict of interest in their responsibilities. In following this guidance, 39% of the respondents noted that they sourced their DPOs internally by appointing to a new role or by adding the DPO responsibilities to an existing role.

In addition, in Article 38(3) the GDPR requires that the DPO reports to the highest management level of a data controller or a data processor. The survey demonstrated that this requirement was interpreted by Irish organisations in a number of ways where 54% of respondents noted that their current or future DPO reports or will report to the Heads of Legal, Risk, Compliance, Operations or HR, and 36% indicated that the DPO will report directly to their CEOs or the Boards.

Insight
Not all organisations are required to appoint a DPO. When this is the case, it is good practice for organisations to assign data protection responsibilities within the organisation. This individual is not an official DPO, but an individual who is to act as an advocate for data protection and privacy and promote lawful, transparent and fair processing of personal data. It is also important to establish a network of privacy champions which can vary depending on the size of an organisation.
Third party contracts
The GDPR imposes a high duty of care upon data controllers in the selection and management of their data processing service providers. Where governance aspects of a processing environment are not clearly defined and implemented it becomes a significant challenge for organisations to successfully implement and operationalise key data protection policies and processes.

Based on the survey, half of the respondents have yet to implement due diligence processes to understand and assess their potential data processors. Interestingly, 58% of respondents indicated that they completed the review of all existing contracts, and 18% of organisations completed the review of the contracts they deemed as posing the highest risk to them.

Insight
Data controllers have to gain comfort around the level of protection given to the data processed on their behalf. To achieve this they have to implement robust and rigorous due diligence procedures to screen their potential data processors. Data controller also have to ensure that appropriate data processing contracts are in place, which meet the requirements of the regulation.

It is also important for data controllers to build strong relationships with data processors and third parties to ensure that they adhere to agreed practices, and support data controllers’ efforts to comply with the regulation.

50% of the respondents have yet to implement due diligence processes to understand and assess their potential data processors.

18% of organisations completed the review of the contracts they deemed as posing the highest risk to them.
GDPR as A Strategic Enabler

Organisations should not see the GDPR preparation effort as a once off project.

Using the GDPR as a strategic enabler rather than a merely another regulation, organisations should take this opportunity and put privacy on their strategic agenda. By developing a privacy strategy, organisations set out long term goals to create a competitive advantage, and provide confidence to their data subjects.

Incorporating an effective data protection by design framework and ongoing GDPR compliance monitoring into “business as usual” practices will support an organisation in creating a privacy conscious culture. Organisations can help build trust with customers by developing a privacy strategy tailored to their business, and building an experience that puts the rights of data subjects at the heart of what they do.

Using the valuable knowledge and experience gained during the preparation activities, organisations should expand these into the long-term vision to define their privacy strategy. Developing and maintaining a privacy mind set is key to ensure that it is built into their corporate culture and business values.

Deloitte Ireland will share insights on how to ensure continuous compliance with the GDPR in the upcoming publications.
At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with approximately 263,900 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has nearly 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte Ireland LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC1499 and its registered office at 19 Bedford Street, Belfast BT2 7EJ, Northern Ireland.

Deloitte Ireland LLP is the Ireland affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2018 Deloitte Ireland LLP. All rights reserved.