How the new General Data Protection Regulation will impact

As has been well publicised, the new General Data Protection Regulation (GDPR) published in the Official Journal of the European Union on 4 May 2016, will come in to force on 25 May 2018. As the implications of the new GDPR are extensive, all businesses dealing with personal data, including financial services providers, need to start now to plan for the new requirements

WHAT'S NEW?

The GDPR has been in progress since 2012 and has gone through extensive debates and changes over the last four years to get to the final text. The new rules aim to protect individuals, by setting out clear rights and requirements, balanced with the need for data processing in business, services and society. As noted in the GDPR recitals: 'The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.'[1]

The recitals also note the impact of technology. 'Rapid technological developments and globalisation have brought new challenges for the protection

of personal data. The scale of the collection and sharing of personal data has increased significantly.'[1]

The GDPR affords flexibility to EU Member States to adopt their own additional rules in some areas, and it is likely that that in each EU Member State there will be the core data protection rules as set out in the GDPR and some additional local requirements.

THE CHANGES

Some of the key changes introduced in the GDPR include new provisions in relation to unambiguous consent, which means that consent needs to be obtained from any individuals whose data you obtain. There are also limitations on the processing of personal data relating to criminal convictions and offences. For some organisations, including insurers, this could have a significant impact, and organisations need to seek guidance from local authorities, including the ICO (UK), and the ODPC (Ireland), to evaluate this area.

There are also changes in relation to subject access request (SAR) timeframes, with a new one month timeframe for providing information (currently 40 days). A useful caveat is that a further 2 months are allowed where requests are complex and/or numerous. A further rule sees standard SARs provided free of charge, however a new provision allows data controllers to charge a reasonable fee where a request is 'manifestly unfounded or excessive', or even refuse to act on the request in these circumstances.

Under data portability provisions, an individual has the right to have personal data transmitted directly from one organisation to another. The capability of firms to provide this will need to be evaluated and solutions implemented.

In relation to privacy statements, these are also extended under the GDPR, and extensive additional information is to be provided to the data subject. This includes:

- The period for which personal data will be stored.
- Details of the rights of individuals including the right to restrict processing.
- The right to withdraw consent at any time.
- The right to lodge a complaint with a supervisory authority, whether the provision of personal data is a statutory or contractual requirement.
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved.

Another potential impact for organisations is where personal data is received from sources other than the data subject. Organisations need to provide affected individuals with a privacy statement within one month, except where this would involve disproportionate effort.

While the GDPR allows member states to implement restrictions in relation to some of the GDPR provisions in specific circumstances, this is limited to privacy notices, SARs, portability and automated decision making, meaning that the other rules cannot have further caveats introduced. Alongside this, Member State law can allow for processing in specific circumstances.

Data protection by design is frequently noted in recent privacy publications, and in this area the GDPR requires data controllers to implement appropriate technical & organisational measures to integrate the necessary safeguards into all processing activities, both at concept and at delivery stages.

CONTINUITY

As at present, data controllers must only use processors who safeguard data appropriately and in line with the regulations, and this must be documented in writing. Under GDPR, both data controllers and data processors need to maintain detailed records of processing activities under their responsibility. These records must contain:

- The name and contact details of the controller.
- The purposes of the processing.
- A description of the categories of data subjects and of the categories of personal data.
- The categories of recipients to whom the personal data have been or will be disclosed.
- Transfers of personal data to a third country or an international organisation.
- The time limits for erasure of the different categories of data.
- A general description of the technical and organisational security measures.

BREACHES & ASSESSMENT

While the Republic of Ireland already has a Breaches Code of Practice, under GDPR a breaches code will be required in all EU member states, with a 72 hour timeframe for reporting. Breaches also have to be reported to the data subject, again this is already in place in the Republic of Ireland.

Privacy Impact Assessments will become mandatory under the GDPR which means that data controllers must carry out assessments of the impact of proposed processing operations on the protection of personal data. This will include projects, products, campaigns, data mining, etc.

Another new requirement is that where processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, a data controller must consult the supervisory authority prior to processing.

Finally organisations operating on a large scale must appoint a data protection officer, with specified tasks under their remit, and a new data protection certification mechanism is introduced in the GDPR, which will enable controllers and processors to demonstrate compliance with the regulations.

So in conclusion, some challenging requirements, and time to get planning! With stronger enforcement, and fines up to €20 million or 4% of firms' total worldwide annual turnover, these are significant deterrents to breaking the rules. ■

Ref: [1] Official Journal of the European Union (2016) General Data Protection Regulation [Internet] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN1

NOTE: This information is for guidance only and is not intended to be definitive or taken as any form of legal advice. You should obtain such independent advice on GDPR as you deem appropriate to your circumstances.

Willa Mawhinney is Head of Compliance for Allianz Ireland, based in Dublin, covering the Irish and Northern Irish jurisdictions. Schedule permitting, she is a speaker at Compliance events and Data Protection conferences. Willa completed her Masters in Business Administration in 2007, focusing on leadership and organisational behaviour, and she lives in Holywood, Co Down.