Crystal Risk Consulting

INSIGHT INTO AN UNCERTAIN WORLD

Briefing note on GDPR

What is it ?

The **General Data Protection Regulation (GDPR)** is a new EU-wide data protection regulation which effectively replaces the **EU Data Protection Directive (DPD)** of 1995 and all related national legislation such as the **UK Data Protection Act (DPA)** of 1998. The GDPR is due to come into force in the UK from the 25th May 2018.

The UK government has confirmed that Brexit will not affect the commencement of the GDPR. Even after the UK has left the EU, GDPR is likely to apply in some form as there is likely to be a need for UK regulations to offer similar protection if UK firms are to be allowed process the data of EU citizens.

Who does it cover ?

The GDPR seeks to protect **personal data** which the European Commission defines as "*…any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

This broadly in line with the DPA though the GDPR is more specific that online identifiers such as IP addresses and location data can also be personal data. Certain types of data such as the genetic and biometric data of an individual are classed as **special personal data** requiring particular care and attention (see Article 9 of the GDPR).

The GDPR applies to **data controllers** who determine the means and purposes of processing and to **data processors** who process this data on the controller's behalf. The definitions of these are similar to the DPA but the GDPR introduces joint and several liability to both data controllers and data processors, with enforcement powers potentially applicable to both types of organisations. Under the DPA, data processors were not subject to enforcement action.

It is worth noting the global reach of GDPR – it relates to any firm which collects personal data on EU citizens regardless of where that firm is based. It also applies to data controllers and processors based in the EU or those offering services aimed at EU citizens. Personal data may not be transferred outside of the EU unless the country it is transferred to has adequate level of data protection (similar to "equivalence" under Solvency II), and/or the organisation receiving the data has adequate safeguards in place to protect the rights and freedoms of the data subject (Articles 44-50).

What does it entail ?

GDPR builds on the DPD but seeks to update it to reflect developments such as modern technology capabilities and cloud computing. It also aims to bring about a greater degree of consistency in data protection regulation across the EU to create standardised responses from Supervisory Authorities to similar infringements, regardless of which country they occurred in. Among the changes introduced by GDPR:

- **Data protection by design and by default** (Article 25) – data protection needs to be an integral part of the design and development of business processes for products and services.
- **Records of Processing Activities (mandatory documentation)** (Article 30) adds new requirements for data controllers and processors to document personal data processing, including identification of data flows, risk assessments, whether it is being transferred outside the EU; how long it should be retained etc..
- **Notification:** Article 33 requires that any material breach of personal data should be communicated to regulators within 72 hours of the breach coming to light. Previously only telecoms and internet service providers had to report breaches. Article 34 requires the breach to be communicated "without undue delay" to individuals affected if the breach poses a high risk to them
- **Data Protection Impact Assessments (DPIAs)** (Article 35) – DPIAs are required where processing is likely to result in a high risk to the rights and freedoms of individuals. These would include where new technologies are being used and/or which involve sensitive data such as the person's health. The data controller will need to assess the risk to individual and cover the security measures that will be put in place to mitigate these.
- **Data Protection Officer (DPO)** (Articles 37-39) – this is a new role required for organisations which process personal data extensively. The DPO will be the first point of contact for regulators on data protection issues and should aim to ensure firms comply with GDPR. While similar to a compliance officer, they also need to have some expertise in IT and data protection to ensure data risks are properly managed across the organisation. The DPO is an important new role: they should have access to adequate resources; be able to act independently; and report in directly to the Board

- **Prior Consultation** (Article 36) requires the Data Protection Officer to consult with the regulator prior to processing data if the DPIA reveals processing which is likely to result in a high risk to the rights and freedoms of data subjects which cannot be mitigated against. The organisation must not process data until the Regulator has given authority to proceed. Once referred, the regulator can invoke any of its investigative or corrective powers set out in Article 58.
- New individual rights including:
    - **Right of Erasure** (Article 17) supplants the right to be forgotten and gives the individual the right to request all personal data relating to them to be erased (subject to certain conditions such as the legal need to retain data).
    - **Right to Data Portability** (Article 20) – the individual has the right to receive some classes of their data their data in a structured, electronic, machine readable format that can then be transferred directly to another data controller or the data subject.

What happens if we don't comply ?

A key change arising from the GDPR is higher penalties for failure to adequately protect data or otherwise comply with legislation. Two separate maxima apply depending on the rule breached:

- Higher of 4% of global turnover or €20m for, inter alia, breach of basic principles for processing (Articles 5-9) or individuals rights (Articles 12-22) – see Article 83, 5.;
- Higher of 2% of global turnover or €10m for other breaches (Article 83, 4.)

These levels will result in significantly higher fines than under current legislation, where the Information Commissioners Office (ICO) can only fine up to a maximum of £500,000[1]. Some studies indicate that fines could increase up to 50x fold[2]. To take an example, in October 2016, TalkTalk was fined £400,000 (= 80% of the maximum) for failing to have adequate cyber defences which resulted in the theft of data on over 157,000 customers[3]. Under GDPR, the equivalent fine could have been 80% of 4% of global turnover which would give a fine of £58.8m. The new fine limits could raise the cost of data breaches considerably, particularly as cyber insurance policies are unlikely to cover such fines.

---

[1] Though the FSA has in the past fined financial services firms more for data breaches: for instance, in 2009 HSBC Actuaries and Consultants Limited and other HSBC firms were fined over £3 million for not having adequate systems and controls to protect customers' confidential details - see http://www.fsa.gov.uk/library/communication/pr/2009/099.shtml.

[2] From a study of ICO fines by NCC Group, ICO fines in 2015/16 were just over £2m but the equivalent proportion of the maxima under GDPR might have been ca.£105m.

[3] See https://www.talktalkgroup.com/articles/talktalkgroup/TalkTalk-Group--moved-articles-/2016/TalkTalk-Group-Q3-FY16-Update and https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack

For banks and insurers, assessments of operational risks and associated capital requirements should have regard to the prospect of higher fines as well as the wider costs of data breaches.

Higher fines are not the only sanctions open to authorities. Article 58, 2. specifies a wide range of powers available to regulators including (f) the right to impose a ban on processing, say if a DPIA indicated a high risk to individual's data. Such a ban, even for a short period, could jeopardise the ability of a firm to continue operating – as such, it should be considered as part of reverse stress testing to identify scenarios which would undermine a firm's ability to remain in business.

Other impacts

GDPR raises the bar in terms of compliance with existing data protection legislation. For instance, where the legal basis for processing is data subject consent, the GDPR introduces a higher quality of consent – i.e. fully informed, freely given, granular and requiring an explicit positive action on the part of the data subject to signify their consent.

Article 22 retains existing legislation[4] around automated decision making and profiling. This gives individuals the right not to be subject to a decision based on automated processing which has a significant impact on them, including the right to request human intervention, to seek an explanation for a decision and to challenge this (though there are restrictions around these rights). This could have a significant impact on those using data science to profile and underwrite individuals for the purposes of insurance or lending.

Another potential problem area is accuracy of records. For instance, Prudential were fined £50,000 by the ICO in 2012 when, having inaccurately merged the records of two customers with the same name, they failed to correct this when the customers highlighted this[5]. GDPR could make such failings even more costly.

What should firms be doing ?

Firms should have in place a program to ensure compliance with GDPR. This should include:

- Documenting data in line with Article 30;
- Carrying out DPIAs where necessary;
- Appointing a DPO where appropriate, ensuring they are adequately supported, and that they have a line of reporting into the Board; and
- Making sure contracts with outsourcers and other suppliers reflect GDPR requirements.

[4] See http://www.legislation.gov.uk/ukpga/1998/29/section/12

[5] See http://breachwatch.com/2012/11/08/prudential-assurance-company/

This program should also review controls around compliance with existing legislation to ensure these are still robust.

GDPR needs to be considered as part of wider information security risk. Recent high-profile breaches at TalkTalk, Anthem[6] and Experian have highlighted the dangers of cyber crime and theft of data breaches.

Regulators are looking for firms to ensure data is adequately protected and that they have adequate cyber defences. For example, in April 2017, the FCA noted that "…*firms continue to struggle to get the basics right*"[7]. They highlighted guidelines such as the ***"10 steps to Cyber Security"*** issued by the National Cyber Security Centre (NCSC)[8] as "good cyber hygiene".

Financial services and other firms would do well to ensure they are adhering to such guidelines at a minimum – failure to do so may constitute a prima facie breach of the basic principles for processing under GDPR, exposing the firm to fines in line Article 83, 5. (higher of €20m and 4% of global turnover) or worse.

Conclusion

A well run firm should comply with most of the requirements of GDPR, but addressing new requirements such as DPIAs and demonstrating compliance will still place a significant burden on firms. Actuaries need to be aware of the increased cost of non-compliance, either in terms of higher fines or, in the worst case, not being able to process data. This adds a further dimension to cyber crime and the cost of data breaches which are an increasing threat to all.

Acknowledgements

Crystal Risk Consulting Ltd. would like to acknowledge and thank Anita Lines Angell, data protection expert, for her contribution in reviewing this briefing note.

[6] A US health insurer who lost nearly 80m active and legacy records in a breach in early 2015, costing ca.US$260m to date - see https://www.digitalcommerce360.com/2017/01/12/regulators-say-foreign-government-caused-anthems-massive-data-breach/

[7] *"Expect the unexpected: cyber security in 2017 and beyond",* speech by Nausicaa Delfas, Executive Director at the FCA, delivered at the Financial Information Security Network, 24th April 2017 – see https://www.fca.org.uk/news/speeches/expect-unexpected-cyber-security-2017-beyond

[8] See https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Links / Resources

GDPR Text http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Other EU links which may prove useful:

http://www.eugdpr.org/the-regulation.html

http://www.eugdpr.org/article-summaries.html

http://www.eugdpr.org/key-changes.html

The ICO have produced a good overview of GDPR which can be found at:

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/