MILLIMAN BRIEFING NOTE

Data protection in a GDPR world

September 2018

Milliman

Overview

The new General Data Protection Regulation[1] (GDPR), which was introduced on the 25 May 2018, strengthens rules regarding the way in which companies use data and should enable individuals to have a greater level of control over what companies do with their personal data.

The GDPR is applicable across the European Union, and as such all UK companies should currently be complying with the regulation. While there are countless papers issued on the legal aspects of the GDPR, few have covered the practical realm of how to design a risk management framework that insurance companies can use for the GDPR and data protection risk analysis. This paper walks you through the high level requirements of the GDPR, but also details specific considerations on the implementation steps.

Data protection is highly important to all types of businesses:

- Collecting, sorting and analysing data is unavoidable, whether it involves handling policyholder data directly, or simply collecting personal data of company employees or clients.
- There is a high price to pay for any error or breach of data, both in terms of direct remedial costs such as regulatory fines and additional staff, or ongoing reputational consequences which damages ongoing business performance.

Using our industry knowledge on data and risk management issues, we provide in this paper an overview of the new GDPR rules, discuss the aspects that firms should consider in light of these changes and explore the implications of the GDPR for a firm's risk management framework. Many of the approaches discussed in this paper could equally be applicable to the management of other types of confidential data.

What type of data can you receive?

Data handling and storage requirements differ under the GDPR according to the type of data received and the purpose for which it is received or stored. For insurers, data stored and received commonly relates to policyholder characteristics or the policyholder's date of birth, name, gender, address, and in some cases, claims/health data. Whilst it is crucial that this data is actively managed to comply with the data protection regulation, it is worth noting that data within the scope of the GDPR is much more wide ranging than policyholder type records. In-scope data also includes any other personal data stored regarding clients, employee candidates or current personnel. Therefore, firms require processes to manage and control the full range of data types they hold, for the full range of purposes for which personal data is handled.

What is personal data?

Under the GDPR, 'personal data' is defined 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, generic, mental, economic and cultural or social identity of that natural person*.[2]"

Pseudonymised data on the other hand is defined differently, but nonetheless should be treated as personal data because it allows individuals to be identified or re-identified. The GDPR defines pseudonymisation as "*the processing of personal data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person*."

Whilst the GDPR relates to personal data, firms should not disregard other types of sensitive data in their risk management processes, as these could also have a damaging reputational or financial cost if not adequately controlled.

[1] The regulation (EU) 2016/679 of the European Parliament and of the Council.

[2] Article 4, Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en.

Data controller vs. data processor

Article 4 of the GDPR defines the different roles as follows:

- **Controller** – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"
- **Processor** – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"

To determine whether an organisation is a controller or processor, it is necessary to find out who is entitled to decide on the purpose and the means of the processing. This determination can vary by project or data type, with organisations being classified as processors in certain instances and controllers in others. Examples of being a controller:

- When an organisation receives personal data from its customers for the purpose of its contract administration or marketing activities.
- When an organisation receives personal data referring to its employees for the purpose of its HR administration.

Example of being a processor:

- When an organisation receives personal data from an entity and is not permitted to process the personal data for its own purposes but rather only under explicit instructions from that entity (usually the data controller).

Data controllers and data processors have different liabilities and responsibilities under the GDPR. It is therefore of utmost importance to know in which capacity they are processing personal data.

We find that working closely with internal and/or external legal counsel is essential in helping all stakeholders to interpret the GDPR and ensuring that all relevant contracts and data sharing agreements (DSAs) are GDPR-compliant.

Data protection impact assessment

Before receiving or processing any personal data, it is necessary for a controller to determine whether a data protection impact assessment (DPIA) needs to be carried out to assess and manage the risks associated with receiving and holding personal data.

A DPIA is required where data processing could result in decisions that have legal or other significant effects concerning a natural person, where data processing occurs on a large scale of special data categories[3] or where there is a systematic monitoring of a publicly accessible area on a large scale. It is generally recommended that a DPIA is carried out for all major projects using personal data.

According to the GDPR, the DPIA should include at least the following:

1. Systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. An assessment of the risks to the rights and freedoms of data subjects referred; and
4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

It is important to note that the DPIA does not necessarily have to be communicated to the supervisory authority. However,

- In cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remain high), then the data controller must consult the supervisory authority;
- Regardless of whether or not consultation with the supervisory authority is required based on the level of residual risk, the data controller is obliged to retain a record of the DPIA and update it in due course; and
- While there is no obligation to publish the DPIA, publishing it could foster trust in the controller's processing activities.

[3] As referred to in Articles 9 and 10 of the GDPR.

Managing personal data under the GDPR

Managing personal data under the GDPR applies at every point in the lifecycle of the data, with key considerations and principles applying at each stage. In our experience, having a robust framework in place and embedding it in business as usual (BAU) processes helps firms to be GDPR compliant without impinging too heavily on other business priorities. From a risk management perspective, it ensures that firms are able to easily assess their exposure to personal data as well as monitor and mitigate the associated risks.

Personal data lifecycle stage	Key considerations
1. Transfer data	▪ The data transfer method should provide a highly secure travel route for the data without leaving the EU. ▪ For example, if e-mail servers or backups are located in non-EU regions, data is technically being transferred outside of the EU even though both the sender and recipient are within the EU. ▪ Consider using methods that encrypt data and minimise the risk of interception. For example, we use solutions such as SFTP transfers or CryptShare. ▪ Once data has been transferred onto the recipient's server it should be deleted from the "in transit" location e.g. SFTP folder.
2. Log data	▪ Personal data should be logged as soon as it is received with the recipient recording key information such as file name, file size, date received, sender's details and transfer method. ▪ Data log files can be managed at an organisation level, team level or project level and should be structured in such a way that each company is able to easily identify and manage all personal data files that it holds. ▪ In our experience, best practice is to extend this process to all data received to ensure that the same principles and processes are applied to managing all confidential data that an organisation may receive.
3. Store data	▪ Access to the data/network should only be granted to employees within the EU who have a valid business need to access it. ▪ Servers and back-ups should be located within the EU with appropriate security and protection measures in place (e.g. fireproof facilities and surveillance). ▪ Appropriate controls and safeguards as well as administrative and physical controls should be in place to provide a high level of security for stored personal data. For example, disabling the use of USB drives on company software.
4. Process data	▪ Processing of personal data relates to any operation or set of operations which is performed on the data. For example, collecting, recording, organising, structuring, storing, adapting or altering the data. ▪ Processing activities should be recorded and records should be made available to supervisory authorities on request. ▪ Processing records will include information such as: data controller and data processor details, purpose for processing data, categories of personal data held, data recipients, time limit for holding the data, technical and organisational measures in place for securing data confidentiality.
5. Retain/ delete data	▪ Prior to transferring any personal data, a data sharing agreement should be in place and signed by all relevant parties that sets out each party's responsibilities with regards to receiving, processing, storing and deleting personal data as well as each party's required actions in the event of a data breach. ▪ Any requirements to delete personal data should be set out in the data sharing agreement, along with a specification of the timeline for data deletion (this could be a specific date or a timeline defined by a milestone such as "project completion"). ▪ Keeping accurate and up to date data and processing logs will improve the accuracy and ease of carrying out this task.

GDPR checklist:

- ✓ Conduct data protection impact assessment (DPIA) if required
- ✓ Signed data sharing agreement (DSA) between all relevant parties
- ✓ Secure data transfer method
- ✓ Data log
- ✓ Secure data storage method
- ✓ Data processing logs
- ✓ Data deletion requirements and timelines specified
- ✓ Responsibilities of all parties specified in the event of a data breach
- ✓ All processes ensure that data is not transferred outside the EU (or region specified by DSA)

Risk management framework

In the context of the above requirements and processes, how can firms update their risk management frameworks to help manage the additional risk exposures relating to data protection in a GDPR world?

Various aspects of the risk management framework can be updated and utilised to manage data protection risks. These include:

- Risk appetite statements on data protection.
- Use of rigorous internally defined processes, coupled with comprehensive employee training, to ensure employees comply with regulation. The nature of, access of and use of personal data are likely to evolve over time, meaning that processes will need to be revisited and reviewed regularly.
- Accurate methods and measurement of the effectiveness of these processes, in order to monitor compliance with the GDPR.
- Using these measurements, a company can then set risk limits. This will allow the company to check compliance, and that the current data protection management is within risk appetite. Companies should consider how strict these limits should be. For example, does the company tolerate a lower level of risk for data breaches compared to other operational risks?
- Additional stress and scenario testing, possibly within a company's Own Risk and Solvency Assessment (ORSA). Considerations may include:
  - Assumptions regarding the breach scenario. For example, considering how long it takes to identify that a breach has occurred, the type and number of customers affected and the costs and time involved in rectifying the consequences of a breach.
  - Calibration of models will need to allow for the large potential fines under the GDPR. Currently, the highest possible fine is the maximum of EUR 20 million and 4% of global annual turnover.
  - Consider how data protection processes could be affected in stressed environments.
  - Are additional controls required as a result of the GDPR?
  - What management actions can be used in case of a breach?
- Board education on the above framework and actions, to provide comfort around the approach to personal data and the GDPR. This can be supported by a gap analysis which would highlight:
  - The regulatory requirements.
  - The actions the company has performed to comply with the regulations.
  - Any improvements to be made, as well as the ongoing monitoring required.

Creative solutions to managing risk

In developing a GDPR-compliant risk framework and associated processes to receive and store personal data, it is important to consider whether personal data is required or if alternative solutions can be employed. Since processing and storing personal data involves extensive security measures and protocols, in some cases we find it is preferable to avoid using personal data and to use anonymised data instead.

For data to be truly anonymised, re-identification of individuals needs to be impossible. For example, if we consider insurance claims data, simply scrambling a member number is not sufficient since you could possibly re-identify a member in the data controller's source database based on the associated claim details if a member was the sole claimant for a particular type of claim on a particular date with particular associated characteristics.

In our experience, technical analyses that use personal data often involve summarising and anonymising the personal data early on in the analysis process. The eventual reported results are typically aggregated data rather than line-level personal data.

To this end and to assist in complying with the data minimisation principle (article 5 of the GDPR), there are some creative solutions that can be considered as an alternative to transferring personal data between organisations:

- On-site data extraction - working together with the data controller, the data processor can arrange to conduct the stages of work that require processing personal data on-site and extract only summaries of the data that are required for further analysis.
- Extract only what is needed - the personal data under consideration will likely contain more detail and be more granular than what is required for the processor's purposes. For example, rather than extract an individual's full date of birth, extract only the age band, age or year/month to reduce the possibility of re-identification.

How Milliman can help

Our consultants have experience in advising our clients on risk management and modelling. We undertake a range of work for clients to enable them to develop their risk management frameworks and manage their data. Our clients know that they can have confidence in us to provide an excellent service and innovative, effective and dynamic solutions that fully meet their needs. We can leverage our industry-leading 'house' approach, which has been developed and refined from our extensive experience of working with clients on risk-related matters, and adapt this to fit clients' unique circumstances.

In the data protection risk management area, we offer assistance with:

- Review of existing risk management frameworks;
- Design and build of operational risk models covering the GDPR risks; and
- Development of risk management frameworks which address data protection risk – for example, developing risk appetite statements and articulating these in terms of risk limits.

If you have any questions or comments on this paper, or on any other issues affecting data protection, please contact any of the consultants below or your usual Milliman consultant.

Milliman

Milliman is among the world's largest providers of independent consulting. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

Milliman maintains a strong and growing presence in Europe with over 350 professional consultants serving clients from offices in Amsterdam, Brussels, Bucharest, Dublin, Dusseldorf, London, Madrid, Milan, Paris, Warsaw, and Zurich.

uk.milliman.com

CONTACT

United Kingdom

Claire Booth
claire.booth@milliman.com

Tanya Hayward
tanya.hayward@milliman.com

Peter Moore
peter.moore@milliman.com