KPMG

The GDPR and key challenges faced by the Insurance industry

February 2018

kpmg.ie

Overview

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) will come into force from 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

This regulation imposes new obligations and stricter requirements on all organisations involved in the processing of personally identifiable data, emphasising transparency, security and accountability.

Objectives

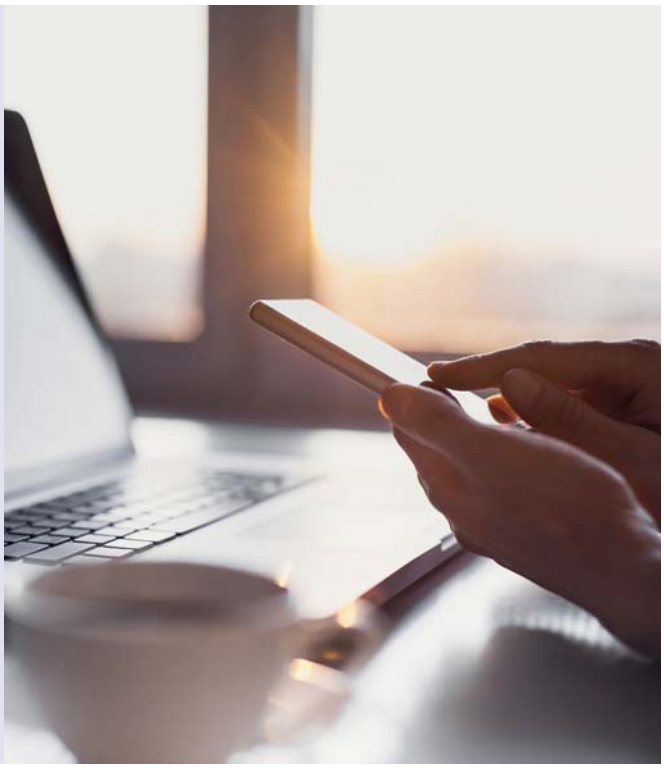
The primary objectives of the GDPR are to:

- Institute citizens' rights in controlling their personal data
- Simplify the regulatory business environment by adopting a unified regulation across the EU

Implications

Failure to comply with the directive may result in:

- Fines of up to €20,000,000 or 4% of total annual global turnover (whichever is greater)
- Reputational risk
- Individuals are also empowered to bring private claims against organisations where their data privacy has been infringed.



GDPR and the Insurance Industry

The introduction of the GDPR is going to have a significant impact on the insurance industry due to the large amount of personal data and sensitive personal data processed by insurers. Insurance companies will need a greater awareness and command over the data they process and share and will also need to be able to justify why they must obtain and hold the data in question. Insurance companies will also now have to deal with the prospect of sharing personal data with competitors in certain circumstances and put processes in place to deal with such requests.

The operational and business impacts of the GDPR will be felt hard in the insurance industry and it's a topic that must be taken seriously given the severity of the potential fines and the risk of damage to reputation. With less than four months to go until 25 May 2018 insurers must dedicate appropriate resources and budget to ensure compliance by the deadline.

Key Challenges Faced by the Insurance Industry

Data portability

One of the biggest challenges that the insurance industry will face is the concept of data portability introduced under Article 20 of the GDPR. Data subjects will now have the right to receive any personal data concerning them, which they have previously provided or has been observed, in a 'commonly used and machine readable format' and have the right to transmit that data to another controller. This only applies to automatic processing, and when personal data is being processed under the lawful basis of consent or performance of a contract.

Not only do insurers have to implement processes to enable them to provide personal data to data subjects and competitors in the correct format within the imposed timelines, they also must have processes in place to receive personal data from competitors. The onus is also on the receiving insurer to ensure personal data received is necessary for the processing purpose and is not excessive. Any personal data received where there is no connection to the purpose of the new processing, should not be retained or processed.

The Article 29 Working Group's Paper on "Guidelines on Data Portability"[1] indicates that portable data processing should be limited to the applicable product and this at least is welcome news for insurers as they will not be required to share confidential business knowledge such as underwriting criteria and risk models.

It remains to be seen how this general process will work in practice and many insurers are of the impression that without a standardised template detailing what information should be shared it will be very difficult to attach any commercial purpose to the data received from competitors. This is mainly due to the fact that different insurers will often have different acceptance criteria for various insurance products.

As pointed out by Insurance Europe *"there may be different types of data that are relevant and not excessive for the different products, which may be challenging for the insurance company receiving the portable data."*[2]

Consent Management

Consent is proving to be one of the biggest headaches for insurers in the context of GDPR, especially relating to the processing of special personal data. Consent can no longer be implied, it must be freely given, specific, informed, unambiguous, clear affirmative and no imbalance of power must exist.

Health data is considered sensitive and collecting it is obviously vital to underwrite and perform numerous types of insurance contracts. Despite much lobbying by insurance groups to include an additional basis for processing sensitive data specifically for insurance purposes, currently under the GDPR explicit consent

[1] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[2] https://www.insuranceeurope.eu/support-expressed-guidance-right-data-portability

appears to be the only legal basis under for insurers to process sensitive data.

This poses a particular problem for sensitive personal data on the current book of business where no consent was received historically. As insurers are currently processing special categories of personal data for both policy holders and third parties, this will make any remediation process far reaching and likely to be extremely time consuming.

The draft Irish Data Protection Bill 2018, which was released on 1 February 2018, appears to offer insurers some welcome relief in the form of a derogation for the processing of data concerning health for insurance where the processing is necessary and proportionate for such a purpose. There are still some open queries with regards to the wording of the bill, hopefully this should become clearer in the coming weeks and months and insurers can anticipate some welcome news in the finalised bill.

Another issue in relation to consent occurs where personal data is currently being processed for minors, where parental consent will be the only basis for processing it under the GDPR, and parental consent has not been received in the past. Insurers may need to adopt an approach to remediate this challenge to a satisfactory level and agree an approach to deal with this going forward to ensure they are still able to process this data and stay in compliance of the GDPR.

Third Party Vendors

It is common place within the insurance industry to have relationships with numerous third parties such as vendors and brokers. Article 26 of the GDPR introduces the concept of joint-controllers where there are two or more controllers that jointly determine the purposes and means of processing. Insurers will need to look at arrangements they have with third parties to determine if this is controller-to-controller or controller-to-processor relationship.

The level of control over the data and whether the entity is involved in decision making relating to the personal data should be a decisive element. It should not just be assumed that if one company provides services to other that this automatically makes them a processor.

It is likely that brokers will be classified as controllers but the insurer must analyse this on a case by case basis to make that determination. It will be important to review and update contracts and agreements with controllers and clearly document the split in compliance responsibilities to avoid dispute in the case of a data breach. In the case of consent where joint-controller relationships exist, it will be important to agree a process for advising the data subject of all controllers and for receiving consent for different aspects of processing.

In the case of processing relationships with vendors it is again vital for insurers to review and update contracts to define roles and responsibilities and to implement appropriate due diligence arrangements to ensure only processers that are GDPR compliant are contracted with.

Transparency Third Parties

Transparency is a key concept in the GDPR with many new requirements have been introduced in this regard. One of the major challenges emerging in the insurance industry is the requirement under Article 14 to provide information where personal data has not been obtained from the data subject. This means where data has been received from a third party, the data subject to whom the personal data relates will now need to be informed of certain details regarding the processing within a set timeframe.

This is likely to cause a major operational burden for insurers as it is common place to process personal data that has not been received directly from the data subject for the proposes of processing insurance contracts. As an example, if a motor insurance policy holder requests that a named driver be added to their policy, the named driver may need to be informed of details relating to the processing including the basis for processing, period retained and details of the controller.

From an operational point of view, this will add complications to the process and make it lengthier, which may frustrate the customer and discourage them from obtaining the service.

Insurers are also likely to have numerous data subjects on their back book of claims and policies that would not have been provided with privacy notices and insurers may need to consider remediating this issue to ensure compliance by 25 May 2018 deadline.

Brexit

As part of their future planning insurers should also be mindful that Brexit is approaching and that transfers to the United Kingdom will become a data transfer out of the EEA. As such appropriate mechanisms will need to be put in place to ensure the transfer is compliant with the GDPR.

How can we help?

It is clear that there are challenging times ahead for insurance companies when braving the new data protection landscape. KPMG have worked with numerous clients across a range of industries helping them get GDPR ready by assisting in the assessment, design and implementation of controls and processes. KPMG'S unrivalled experience of large transformational change projects means we understand the challenges facing you and can assist you in addressing them.

From a regulatory viewpoint KPMG have vast experience working with both life and non-life insurance companies, providing advice and helping implement new regulatory requirements.

KPMG has a breath of understanding relating to the insurance industry and the requirements of the GDPR and can help you meet general challenges and challenges specific to this industry.

In particular, KPMG can assist as follows;

- Review any gap analysis and any risk assessment completed to date between your company's existing data protection processes and the GDPR;
- Help create and collate personal date registers;
- Assess your company's GDPR Readiness state;
- Identify weakness and help your company work through any problematic or high impact areas;
- Work with your company to put a detailed project plan in place to ensure compliance ahead of the deadline;
- Assist with the design and implementation of revised data protection governance structures;
- Help with the roll out of staff training and awareness throughout the business; and
- Assist with the implementation of an on-going monitoring programme to demonstrate compliance.

Contacts

Brian Morrissey
Partner

T. +353 1 410 1220
E. brian.morrissey@kpmg.ie

John O'Donnell
Director

T. +353 1 700 4251
E. john.odonnell@kpmg.ie

Niamh Mulholland
Director

T. +353 1 700 4785
E. niamh.mulholland@kpmg.ie

Aine McPartlan
Manager

T. +353 1 700 4832
E. aine.mcpartlan@kpmg.ie

kpmg.ie

Produced by: KPMG's Creative Services. Publication Date: February 2018 (3598)