http://www.pwc.co.uk/fsrr

Stand out for the right reasons

Getting insurers ready for the GDPR

The General Data Protection Regulation (GDPR) and its impact on insurers

May 2016

pwc

The General Data Protection Regulation (GDPR) and its impact on insurers

In 2018, the European Commission will mandate the General Data Protection Regulation (GDPR), centralising regulation across the 28 member states of the European Union and updating it for the digital age. Any entity targeting or monitoring European citizens will need to be compliant. This is a big shake-up, and will cause significant disruption to how insurers store, manage and process personal data.

The GDPR in a nutshell

The European Commission has approved the final text of the GDPR. From May 2016 Insurers will have a two-year window to ensure compliance. The challenge now is for insurers to see the GDPR as an opportunity to be embraced, as well as a challenge to overcome.

So, what is changing?

- ***Data breach deadlines***
  Insurers will have just 72 hours to disclose a personal data breach to the regulators, and in some cases to the affected individuals.
- ***Better quality consents required***
  Insurers will have to meet tougher quality requirements for legal consent, if they want to rely on consent to process personal data. Customers must give that consent freely and on the basis they have been fully informed about the nature of each type of usage. The insurer will have to be able to prove that they have obtained consent of the right quality.
- ***Privacy by design***
  Insurers will be required to minimise the collection and use of personal data – and will be expected to do this automatically as they design new products and services.
- ***New fines and penalties***
  Regulators will have the power to fine insurers up to €20m or 4% of worldwide annual turnover (whichever is higher) for the most serious breaches of data protection laws.
- ***Processing now at risk***
  Customers will have the right to object to having data on them used for insurance activities such as risk and pricing modelling unless the insurer has compelling and legitimate reasons for doing so. Customers have the right to object to data processing for direct marketing.
- ***Profiling gets tougher***
  Insurers won't usually be allowed to make decisions about customers purely on the basis of automated processing, including profiling, unless they have established a legal right to do so, which will generally be contract-based.
- ***New right to be forgotten***
  Customers will be entitled to ask insurers to delete their personal data where it is no longer required for its original purpose, or where they have withdrawn their consent.
- ***Portability guaranteed***
  Customers will be entitled to request that their personal data is transferred from one insurer to another as they switch companies. Insurers will be obliged to facilitate this.
- ***International data transfers***
  While EU data transfer rules are not fundamentally altered, there will be enhanced regulation of the mechanisms put in place to ensure that personal data is properly protected when abroad.
- ***Data protection officers***
  Some commentators are interpreting the GDPR as requiring the compulsory employment of Data Protection Officers (DPOs) in the insurance sector. PwC considers that DPOs are required as a matter of good governance in all cases.

Did you know?

Guaranteed data portability

Under GDPR, your customers can request for their personal data to be transferred from you to a competitor.

Data portability

If you have a data breach you will have 72 hours to report it. Fines for non-compliance of the GDPR, could be up to 4% global annual turnover

The right to be forgotten

Under GDPR, your customers will have the right to ask you to delete their personal data.

How will the GDPR affect you?

The regulatory imperative of GDPR creates some very specific issues for insurers, and the cost of non-compliance will be very high, both in terms of potential fines, and broader reputational damage.

For example, meeting a 72-hour deadline for full disclosure of a data breach will be impossible for companies that do not have an incident detection mechanism and escalation process to be able to report exactly what has been breached. Insurers will also need to be ready to transfer a customer's data to a new provider, or to delete it if requested. To be able to achieve this, insurers will need to have response processes and know where their data is.

Similarly, the requirement to obtain better quality consents, even from existing customers for data processing, will represent a major headache. Some will require a significant cultural shift. For example, as new customers are acquired, and products and services developed, insurers will need to take the likes of 'privacy by design' and the 'right to be forgotten' into account.

The broader concern is that the GDPR threatens insurers' innovation pipeline – and even their ability to compete. There is a distinct threat that greenfield entrants to the insurance sector who are not constrained by legacy burdens, can build their systems from scratch and be GDPR compliant from day one.

Still, insurers do need to see the GDPR as an opportunity to be embraced as well as a difficulty to be overcome. The system and process renewal necessitated by the new regulation may prove to be a positive as insurers seek to innovate at speed. Combining the compliance effort with the drive to obtain competitive edge from data and analytics will leave Chief Data Officers (CDOs) and their teams with no choice but to embrace customer-centricity. Those insurers able to secure data advantage may come to regard the effects of the GDPR as benign – or even as positive.

What are the next steps?

Insurers must now move swiftly to solve the problems posed by the GDPR and to capture the opportunities it creates.

First thing's first

Insurers must initially assess where GDPR sits within their risk appetite, and look at the opportunity it could pose. They will also need to carry out an assessment of their current state as it relates to the new regulation. Most organisations have a lot to do to close the gaps and we suggest a risk-based approach to becoming compliant. A risk-based approach takes into consideration the specific characteristics of an organisation (e.g. the type of personal data, the nature of the customer interaction, geographic operations etc.) and places those elements alongside the gaps and the risk appetite.

Following the assessment and prioritisation phases, organisations may need to carry out one or more of the example activities listed below:

Find out what you have and where it is

The urgent priority for insurers is to identify exactly what data they already have, and how and where this information is stored. This will apply both to existing data storage, which may be spread across myriad systems, held in different forms and often poorly reconciled – and to new data, as it comes into the organisation.

A key part of this auditing process will be understanding what consents and permissions have been obtained for each element of data held. Where those consents are lacking or insufficiently explicit under the GDPR, it may be necessary to contact customers in order to obtain the right permissions.

At the end of this first stage of the response, insurers should:

- understand what data is held, where it is and who has access to it
- have a clear view of any additional risks posed by third-party access to data
- be sure that data is being used only in ways that customers have consented to
- know how well their data is protected.

Consider how you currently use data across your business – and how you would like to use it.

Insurers use data in different ways in different functions and many are pioneering innovative tools and technologies with the potential to reduce cost, limit risk and boost revenue growth. Now they must look at every use-case for their data (both current and in development) in order to establish what remains viable, and what needs to change under the GDPR. That process must take place in every function, including the examples below.

Claims
Insurers are already using data and analytics tools in the battle to reduce fraud – for the benefit of all – and there are further opportunities to explore; might social media provide valuable evidence of fraudulent claims, for example? However, the new regulation on the consent required for data processing may pose a threat to this work.

Pricing
Insurers are excited by the potential of telematics to help them price policies on a much more bespoke basis. The new regulation will limit how telematics data can be used without consent – it will certainly become much harder to monetise this information.

Underwriting
Rich data enables insurers to identify smaller and smaller homogenous pools of risk, particularly by bringing in non-traditional insurance data such as customers' credit histories and health records – and even data from geo-location tools. The extent to which customers will give their consent for such data under the GDPR is unknown. Valuable health data may be a particularly knotty issue.

Marketing
Marketing is increasingly dependent on highly sophisticated data and analytics tools, capable of delivering personalised messages to customers – boosting acquisition and retention. It may become a lot harder for insurance marketers post 2018, as the GDPR affords customers the right to object to the use of personal data for direct marketing. And where international insurance groups seek to share information across the company for cross-selling purposes, the new restrictions on data transfers may be problematic.

In each of these functions, and across the business, insurers will need to evaluate whether what they currently do – and what they hope to do in the future – is acceptable under the GDPR. This will determine whether new consents and disclosures are required, or whether certain activities will simply be off-limits.

At the end of this second stage, insurers should:

- have an organisational view of what data privacy means to the whole business
- routinely be incorporating data protection and privacy issues into overall business strategy
- be confident that their systems and processes are agile enough to facilitate innovation
- be ready for further change as the regulatory environment evolves.

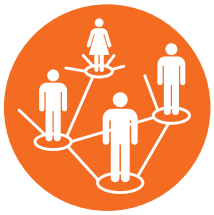
How can PwC help?

- We can help demystify what data protection and privacy is, (including its implications and associated requirements) by working with you to understand how it impacts your organisation, both today and under the GDPR.
- You can complete our Readiness Assessment Test, helping you to identify weaknesses and gaps.
- We can give you access to a global, multidisciplinary team that encompasses risk assurance, legal and forensics capabilities with cross-sector expertise.
- Our team can help you to develop a strategy for privacy investment, and suggest approaches for the management of privacy, including roles and responsibilities, governance and reporting.
- We will show you the threats most relevant to insurance, and can help you identify what matters most to your organisation, where it is, and who has access to it.
- Bespoke training can ensure your employees and suppliers are properly engaged, trained and aware of their duties.

Stand out for the right reasons

Alert

Protect



Adapt

Repair

Financial services risk and regulation is an opportunity.

At PwC we work with you to embrace change in a way that delivers value to your customers, and longterm growth and profits for your business. With our help, you won't just avoid potential problems, you'll also get ahead.

We support you in four key areas.

- By alerting you to financial and regulatory risks we help you to understand the position you're in and how to comply with regulations. You can then turn risk and regulation to your advantage.
- We help you to prepare for issues such as technical difficulties, operational failure or cyber attacks. By working with you to develop the systems and processes that protect your business you can become more resilient, reliable and effective.
- Adapting your business to achieve cultural change is right for your customers and your people. By equipping you with the insights and tools you need, we will help transform your business and turn uncertainty into opportunity.
- Even the best processes or products sometimes fail. We help repair any damage swiftly to build even greater levels of trust and confidence.

Working with PwC brings a clearer understanding of where you are and where you want to be. Together, we can develop transparent and compelling business strategies for customers, regulators, employees and stakeholders. By adding our skills, experience and expertise to yours, your business can stand out for the right reasons.

Contacts

For additional information please contact:

Michel Abbink
Partner, Insurance Actuarial Services Practice
M: +44 (0)7715 484353
E: michel.abbink@uk.pwc.com

Paul Delbridge
Partner, Insurance Actuarial Services Practice
M: +44 (0)7711 563272
E: paul.p.delbridge@uk.pwc.com

Daniel Cole
Partner, Insurance Consulting Practice
M: +44 (0)7740 894685
E: daniel.cole@uk.pwc.com

Craig Skinner
Director, Risk Assurance Data
M: +44 (0)7734 974406
E: craig.skinner@uk.pwc.com

160516-123625-JA-OS