The Insurance Institute of Manchester
Chartered Insurance Institute

The New Class 2016-2017 Report 1: General Data Protection Regulation (GDPR)

What does GDPR and the new Data Protection Act mean to Insurers?

General Data Protection Regulation (GDPR)
The effect on Brokers/Intermediaries

Contents

Meet The New Class

During the summer of 2016, the Insurance Institute of Manchester was inundated with applications from candidates eager to achieve a place on ‘The New Class 2017’ programme.

From a number of applications only twelve successful candidates were selected to participate in a tailored training programme, to help them develop both themselves and the industry.

The group was then split in to two teams and had to utilize the skills learned during the year to create a report based on the implementation of the new General Data Protection Regulations.

The following report has been created by:

Daniel Palfrey
RSA Group

Tom Edwards
Kellands (Hale) Ltd

Nicole Duffy
HSB Engineering Insurance

Andrew Agoston-Jones
Bollington Insurance Brokers

Josef Horrocks
Marsh

Rebecca Mlota
Finch Employee Benefits

With Assistance from Stephen Bridge, Zurich

Introduction

This report aims to offer an exploration into the General Data Protection Regulation (GDPR) [1], which comes into force May 25th 2018.

We will specifically look at the impact this will have to the insurance industry, touching on both commercial and personal lines insurers.

We will be looking at the main differences between the current Data Protection Act 1998 (DPA '98) and the GDPR and how this relates to the industry.

It is important to note that this report is not a thorough evaluation of the changes the GDPR will bring but instead a summary of some of the main features.

Why we need a change

Although the Data Protection Act was updated in 2003, it is still insufficient to cover the huge amount of recordable and usable data we generate every day. The GDPR will take into account how we live in a truly online society.

When DPA '98 became law, less than 10% of households had an internet connection, and Google had not yet been launched. It is now possible for our smartphones to record what we say and search for, and for this data to be stored and assimilated into an online profile without us ever being aware.

The constant stream of data we all generate on a daily basis potentially leaves us open to new threats, whether that be via cybercrime such as phishing or fraud, or sensitive information being sent to the wrong recipient.

In a modern society of targeted advertising online, location tracking and Big Data, a legislative overhaul was required in order to protect people from having their data exploited in ways they hadn't agreed to.

Current Data Legislation

The UK currently follows the rules outlined by The Data Protection Act 1998 and offers guidelines around how personal data is collected, managed and used by third party organisations. The Data Protection Bill, published in September 2017 is an enhancement being used to clarify any grey areas in the UK.

The Key principles of DPA 98 are still embodied in the GDPR so let us begin by refreshing our memories with what those are. The current DPA principles are as follows:

1. Personal data shall be processed fairly and lawfully

Principle 1 requires that consent for processing of sensitive data must be explicit, and not just assumed. There are however exceptions regarding the interests of National Security, taxation or domestic purposes

2. Personal data shall only be obtained for a specified lawful purpose

Principle 2 aims to promote transparency of the firm's motive for keeping the data in question

3. Personal data shall be relevant, adequate and not excessive

Principle 3 ensures the data held is reasonable and not excessive

4. Personal data shall be accurate and up to date

Principle 4 demands that data be kept up to date and accurate

5. Personal data shall not be kept for longer than necessary

Principle 5 describes how long data should be reasonably kept for and how it then be destroyed once that period has ended

6. Personal data shall be processed in accordance with the rights of data subjects

Principle 6 is multifaceted as it looks at the rights of the individual to access, restrict the use of or amend data held on them

7. Appropriate measures shall be taken against unauthorised or unlawful processing and against loss.

Principle 7 describes guidelines for protecting a client's data

8. Personal data shall not be transferred to a country or territory outside the EEA unless that country ensures an adequate level of protection of that data.

Principle 8 outlines the premise on which data may be shared internationally.

What has changed

GDPR makes the controllers more accountable by amending current regulatory processes, and introduces a far reaching and more punitive regime for breaches and errors. It also makes controllers more accountable to subjects, who will have greater control over their data. So what will change with the roll out of the GDPR? The main differences between the current DPA 1998 directive and the GDPR are summarised below.

Regulation vs Directive

GDPR is an EU regulation, whereas DPA is a directive [8]. A directive states an aim, and member states can pass whatever laws they feel they need in order to meet this aim. A regulation is passed by the EU parliament and is enacted into law in its existing format with immediate effect, superseding any local laws. Although the UK will no longer be a member state after Britain exits the EU (Brexit) GDPR will still apply.

Increased territorial scope.

The extended jurisdiction under GDPR applies to all companies processing the personal data of anyone residing in the EU, regardless of their location. Non-EU businesses processing EU relevant data will have to appoint a representative in the EU. A separate Data Protection Directive is being issued for the Police and criminal Justice sector.

Penalties

The maximum fine for a breach has also seen a significant increase. Previously this had a cap of £500,000 as this was deemed a significant and meaningful amount to act as a future deterrent. This has now been increased under the GDPR and fines can be up to 4% of global turnover or 20million Euros.

Consent

Requests for consent must be given with transparency and the purpose of the need for the data made clear. Consent must be clear and distinguishable from other matters and not hidden in long T&C's. It must be as easy to withdraw consent as it is to provide it. You can see the changes to this on many sites now, with companies pro-actively moving to an 'opt in' approach to marketing and data collection.

Breach Notification

The guidelines around a company's breach notification process have also been tightened under the GDPR. It is now the duty of a company to notify of a breach where it is likely to 'result in a risk for the rights and freedoms of individuals' in less than 72 hours of first being aware of the breach. Data processors will be required to notify their customers and the controllers, 'without undue delay' after becoming aware.

Right To Access/Erasure

Subjects have the right to obtain confirmation of data storage, how it is being processed and the reason why. This must be provided free of charge in an electronic format. Conversely, a subject can have the controller erase their data, cease further dissemination of the data and potentially stop third parties processing the data. Reasons for this could include no longer being relevant or

withdrawing consent. This is in relation to 'public interest', not that of the controller. Citizens now have the right to question and fight decisions that affect them that have been made on a purely algorithmic basis

Portability

An individual, under the GDPR, will have the right to move any data collected by automated means to another firm without being prevented from doing so by the previous firm. This must be provided in an open standard, making it accessible by the new controller. However this only relates to data given by the individual, not any manipulation a controller may have applied.

Privacy by design

When developing new software or a new system, data protection considerations must be included from the very start and not an add-on or after thought. GDPR states 'The controller shall … implement appropriate technical and organisational measures … in an effective way … in order to meet the requirements of this regulation and protect the rights of Data subjects'. The Regulation calls for controllers to only hold and process data absolutely necessary for the completion of its duties (data minimization) as well as limiting access to personal data to those needing to process it.

Data Protection Officers

Under DPA 98, controllers are required to notify activities with local Data Protection Authorities, which can be subject to different laws and processes in different member states. Under the GDPR there will be internal record keeping requirements and for some firms a mandatory Data Protection Officer (DPO) who's main function is compliance within the GDPR. They will in effect act as an internal regulator, standing semi-independently from the company they are employed by, in a similar function to a compliance officer. Their knowledge will need to extend beyond Data Protection Laws, and into business continuity and managing IT processes to guard against cyber-attacks.

Things to Consider

Hiring of a full time Data Protection Officer

Once GDPR is passed into law large firms will be required to have a Data Protection Officer who will report directly into the top level executives of the company. This new role also comes with additional protections and almost sits externally to the company, so be aware when appointing into this role. The role of a Data Protection officer involves process implementation, ongoing training and continual development in order to maintain required standards of compliance and data control.

Under GDPR, a Data Protection Officer needs expert knowledge of data protection law.

It is worth noting that the DPO will only offer advice and will not act or implement these changes themselves. It is the responsibility of the organisation to follow their advice to ensure GDPR compliance.

Although the job title and job description may be new, most large insurance companies will already have a dedicated department whose roles and responsibilities are based on DPA compliance. Aligning to the GDPR should not be seen as something to be concerned about to those large insurance companies who already take care with their customer data.

Consent

You may note that when reading online many articles focus on clarity around consent. However, as an insurer who is in a legal contract with our customers we have the right to use that data for the purposes of the business within that contract period. As an insurer we will also have a business relationship with our customers and as such can contact them via using personal data such as emails. Where insurers may need to worry about consent is when thinking of how they market to new or potential customers and ensure the data they are using was gathered with clarity.

Data Projects and Profiling

A key component of the underwriting process is using vast amounts of consumer data to generate rates and in turn premiums for the end customer. The GDPR notes that purely automated processes should be discouraged due to the potential for unfair treatment of the end consumer.

However, as previously mentioned, due to the data used by insurers being the product of a legal contract no changes to processes need to be changed. The profiling used by insurers also has underwriter input and as such the process is not purely automated and can be reviewed to suit individual needs.

One area that may be worth looking into in more detail is the shift to purely automated process within the SME insurance industry.

Breach Notification Mechanisms

GDPR amends the regulation surrounding the notification of breaches. Under GDPR, companies may be required to notify their ICO without undue delay and, where feasible, not later than 72 hours after

having become aware of a breach. Firms will also be required to notify the individual concerned if there is a high risk to their rights and freedoms. The new onus of notification which is being placed upon insurers means they may need to review their breach notification process, with the DPO having a central role in this.

Again, as mentioned, many large insurance companies already have detailed breach notification and quality assurance systems in place and adhering to the stipulations within the GDPR should not have too great an impact.

Data Auditing

Be confident that as an insurer your use of consumer data is in line with the contract on which it is based. Having clear systems and processes that audit and check data is being handled and manipulated correctly will allow for a smooth GDPR transition.

J D Wetherspoons recently took drastic measures to avoid the need for a data audit and deleted all held customer information. Going forward this will ensure that all the data they collect is done through clear means and with informed consent. Now, insurers will not need to take such a drastic stance, but this highlights one of the lengths a business will go to in readiness for the GDPR.

Due Diligence

Insurers may need to confirm that the brokers they work with have the correct measures in place to prevent a data breach and to deal with any breaches should they occur. Speaking to a local insurance implementation manager it is clear that this is something already in place within their company but is an area now receiving more focus.

Within commercial insurance, there is a sector that hands over the pen (underwriting) to the broker for them to write on the insurers behalf. This area of insurance is one that is already strongly regulated and thorough due-diligence around this field is an industry must. In order to satisfy the FCA an insurer must be able to clearly demonstrate that the delegation of underwriting is only given to brokers who have proved they sufficiently adhere to industry standards.

The transition from the Data Protection Act 1998 to the GDPR requires that this due diligence can be proven on demand. Evidence of a broker's practices will need to be evidenced and their own compliance department will need to provide sufficient resources to demonstrate what they are doing to ensure they are operating in compliance with the new regulations. This will encompass how data is collected by the broker, how it is stored, how long it is kept and how they have obtained consent to marketing. To strengthen broker relationships and aid with due

diligence insurers could share their resources with those they are delegating to ensuring both entities are following similar practices.

Data Portability

The right to data portability enables individuals to obtain and reuse personal data collected by automated means.

Insurers will need to comply by ensuring that the information is provided free of charge in a structured, commonly used and machine readable format. This is so that the data is easy for the new controllers to process.

As noted earlier, insurers will not need to supply any data that has been manipulated or translated into a usable format. It is the responsibility of the new controller to use the data they receive.

Underwriting Impact

An insurer will have to be vigilant in ensuring customer information is protected from both internal and external misuse and that only those individuals who are meant to, have access to the data. Misuse will also apply to legitimate marketing and use of data for profiling such as using credit scores to presume a client's personality. Cyber-attacks are a potential threat to firms and there may now be a larger opening in the market for insurance companies to sell cyber insurance to their clients which will help them if a cyber-attack occurs.

Conclusion

There is no doubt that the new regulations will bring about some welcome reforms to an outdated act. As we have mentioned earlier, the world is not the same today as it was in 2003, 1998 and especially 1988, so the opportunity to make your business and client data secure in the 21st century should be embraced.

At first glance this report suggests a lot of work needs to be done to be ready for May, which may be true in some cases, however companies that already adhered closely to the Data Protection Act will probably notice only subtle changes are required to bring their compliance up to date.

The first thing we recommend is that you set aside some time in the near future to review the data journey within your business.
Take a new client enquiry for example:

- How is that information received?
- Where is it stored?
- Who accesses that data?
- How is it secured?
- How is that data used?
- What happens when that data is no longer required?

By following this process you will start to get a clearer picture as to how much work will be involved. You can then start to look at the procedures in place for data breaches, training of staff and regular audits. The worst thing anyone can do is to bury their head in the sand and hope it'll just sort itself.

Failure to adapt quickly could cost Insurers, not just in the fines we have outlined but more long term with the damage to their reputation. How many computer gamers trust SONY with their account information now, following their staff and client data breach in 2015 and most recently again in February 2017?

Don't be afraid to promote how your company is embracing the changes, both brokers and customers will appreciate the extra efforts you, as insurers, are making to secure their data.

There is plenty of help and advice out there, from legal firms, the CII and BIBA, a simple google search can also bring up pages and pages of advice. What we have done here is to highlight the key areas we feel will be impacted by the changes and what sort of changes may need to be made by insurers over the next few months.

Bibliography

1. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3265-1-1
2. http://www.computerworlduk.com/security/brexit-gdpr-why-leaving-eu-will-make-life-harder-for-enterprises-3641825/
3. http://www.eugdpr.org/key-changes.html
4. http://webarchive.nationalarchives.gov.uk/20160109012432/http://www.ons.gov.uk/ons/dcp171778_275775.pdf
5. https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions
6. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/
7. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-Data Protection Officer/
8. https://iapp.org/news/a/podcast-how-to-interpret-the-new-gdpr/
9. https://www.pwc.co.uk/industries/financial-services/regulation/are-you-ready-for-the-general-data-protection-regulation.html
10. https://www.dacbeachcroft.com/en/gb/articles/2016/june/gdpr-deep-dive-profiling-in-the-insurance-industry/
11. https://teiss.co.uk/news/wetherspoons-customer-data-gdpr/?getcat
12. http://www.insurancecompliance.co.uk/latest.news.general.insurance.compliance.shtml
13. http://www.eugdpr.org/eugdpr.org.html
14. https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf
15. http://www.nig.com/news-and-views/2017/smes-braced-for-sweeping-data-protection-overhaul/
16. https://united-kingdom.taylorwessing.com/globaldatahub/article-compliance-burden-under-gdpr-data-protection-officers.html
17. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/
18. http://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation;
19. https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf
20. https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation
21. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-object/

General Information

Address: The Insurance Institute of Manchester
Barlow House
Minshull Street
Manchester
M1 3DZ

Tel: 0161 236 2926
Email: lii.manchester@cii.co.uk
Web: www.cii.co.uk/manchester
Twitter: @IIMPresident
LinkedIn: Insurance Institute of Manchester

General Data Protection Regulation (GDPR)
The effect on Brokers/Intermediaries