The New Class 2016-2017 Report 2: General Date Protection Regulation (GDPR)

What does GDPR and the new Data Protection Act mean to Brokers/Intermediaries?

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

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 utilise 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:

Andrew McDermott
RBIG Corporate Risk Services

Beth McNeil
RSA Group

Daniel Astle
Marsh

Sowmya Nandala
Co-op Insurance

George Anderson – HSB Engineering Insurance

Scott Paterson – Alan Stevenson Partnership

With Assistance from Katie Jackson, Bollingtons

Introduction

It is important to recognise that this report is an overview of the GDPR and how the new law may affect insurance brokers. As organisations vary in size and complexity this report is for brokers to consider the impact to them and is not specifically designed to advise on specific practices to be implemented.

This is not a comprehensive review of the act and is merely an overview.

This legislation has taken more than four years from the publication of the first draft of the Regulation in January 2012 but the General Data Protection Regulation (GDPR) was finally approved by the EU parliament on 14 April 2016.

With the main purpose to replace and modernise the current Data Protection legislation.

GDPR will become law 20 days after its publication in the EU Official Journal and will be directly applied in all EU Member States two years after this date.

Enforcement date - 25 May 2018.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. As a broker the GDPR requires you to demonstrate compliance with the principles.

Overview of the current rules

The Data Protection Act 1998 controls how personal information is used by organisations, businesses and the government.

Everyone responsible for using data has to follow strict rules called 'data protection principles'.

They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for personal sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Why do we need a new regulation?

The need for the change from the Data Protection to the GDPR reflects the changes in technology and the way organisations collect information about people. Since the introduction of the current law there has been an increase in computer usage, and internet traffic has increased exponentially in this time. Over this same period the insurance industry has also adapted to keep up with the times and now more and more insurance transactions are carried out over the internet: from direct quotes to insurance aggregators.

The modernisation of the existing legislation brought about by the GDPR is necessary to better safeguard the data which is collected and now the individual must be aware of exactly how their data will be used going forwards.

Will Brexit have an impact on the GDPR?
Following the EU Referendum on the 23rd June 2016, and the UK's decision to leave the EU, the government has confirmed that this will not affect the introduction of the GDPR.

Information Commissioner's view:

"The fact is, no matter what the future legal relationship between the UK and Europe, personal information will need to flow. It is fundamental to the digital economy. In a global economy, we need consistency of law and standards – the GDPR is a strong law, and once we are out of Europe, we will still need to be deemed adequate or essentially equivalent."

Elizabeth Denham, Information Commissioner

Overview of the Main Changes

Individual Rights
The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA:

Right to be Informed
The right to be informed emphasises the need for transparency over 'fair processing information' or how organisations will use personal data. This will likely be in the form of a Privacy Notice.

What is the impact to an Insurance Broker?
The GDPR will mean Brokers will need to be more transparent about how data is collected and processed.

In addition, it is likely that existing Privacy Notices will have to be amended to include the following:

- Your full company name and contact details
- Details of any businesses processing the subject's data
- The purpose and legal basis for processing the data
- The legitimate interests of the data controller or third-party data processor
- Notification of each of data subject's rights (see below) including the right to withdraw consent at any time.

A Terms of Business document will no longer be sufficient to inform a client of these details

Right of Access
The purpose of the Right of Access under GDPR is to allow individuals to access their personal data so that they are aware of and can verify the lawfulness of the processing.

What Information is an individual entitled to?

Under the GDPR, individuals will have the right to obtain;

- Confirmation their data is being processed
- Access to their person data
- Any other Supplementary Information – which mostly corresponds to the information provided in a privacy notice

What is the impact to an Insurance Broker?
Under the GDPR, this information must now be provided free of charge, and now must be provided without delay and within 1 month of the request at the latest

However, a 'reasonable fee' can be charged when a request is excessive and particularly repetitive.

GDPR states that the information should be provided in a commonly used electronic format. Brokers should consider file formatting and consistency when this information is requested, as systems may have changed since the client was first taken on and a request for this information could be time consuming and costly.

Right to Rectification:

Any individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

This right reflects the existing right, and explicitly states, having regard to the purpose for processing the personal data; individuals have the right to obtain completion of incomplete personal data.

What is the impact to an Insurance Broker?

In the event of a change being made by a client, it is the broker's responsibility to notify any appropriate third parties of these changes.

The broker must also make the client aware of the third parties which need to be informed of the rectification of data.

The right to be forgotten

Is also known as 'The right to erasure'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

What is the impact to an Insurance Broker?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

An Insurance Broker can refuse to comply with a request for erasure if the data is necessary for the performance of an insurance contract (even after it has expired).

How does the right to erasure apply to children's personal data?

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

The right to restrict processing

This gives the individual the right to 'block' or suppress processing of personal data.

What is the impact to an Insurance Broker?

This means that if the broker has the right to store the personal data, but no longer allowed to further process the information. This is unlikely to be relevant to an insurance broker as they would no longer be able to process the insurance if the individual blocks processing.

The right to data portability

Allows individuals to obtain and reuse their personal data, provided it has been collected by automated means, for their own purposes across different services. It allows the individuals to transfer this type of personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

What is the impact to an Insurance Broker?

This is only likely to affect insurance brokers if they collect information using telematics or other automated devices.

The right to object

Individuals have the right to object to –

- processing, where it is based on consent; and
- direct marketing (including profiling)

What is the impact to an Insurance Broker?

There is no significant change as individuals already have the right to object to direct marketing

Rights of automated decision making

Under the new GDPR regulations individuals have the right not to be subject to a decision which has been based on automated processing and if it produces a legal effect or a similarly significant effect on the individual.

This right does not apply to all automated processes.

What is the impact to an Insurance Broker?

Brokers must ensure that individuals are able to, obtain human intervention, express their point of view; and obtain an explanation of the decision and challenge it.

Rights on profiling

The GDPR defines profiling as any method of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

What is the impact to an Insurance Broker?

Brokers who process personal data for profiling purposes, must ensure that appropriate safeguards are in place.

These include:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use of appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Key Considerations

Awareness

Brokers should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Training

As well as decision makers and key people in their organisations, it is important that the rest of the organisation understands the impact that the GDPR will have on their work activities. Brokers will need to ensure that their compliance training is reformatted to ensure they are complying with the GDPR. A 'tick box' exercise will no longer suffice and instead the organisation will need to demonstrate that their employees understand the new process that will be implemented in order to comply with the GPDR. Already there are several companies offering compliance training to businesses.

Data Protection Officers (DPO)

If a broker has not already appointed a DPO, then this may be something they can consider, however most brokers are unlikely to require a formal Data Protection Officer. It may be that existing compliance officers can take on the role of data protection manager, but brokers should avoid calling them a DPO. It is most important that someone in the broker's organisation, or an external data protection advisor, takes proper responsibility for data protection compliance and has the knowledge, support and authority to carry out their role effectively.

A DPO needs to be appointed if a broker;

- carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

The Data Protection Officer's minimum tasks are as follows;

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is being processed.

Information you hold

GDPR has promoted an accountability principle for all organisations who hold personal data. It is important that information is organise, and records are kept as to where it has come from and who it has been shared with. Brokers will need to maintain careful records of processing activities.

Lawful basis for processing personal data

For processing to be lawful under the GDPR, firms need to identify a legal basis before they can process personal data, this then needs to be documented.

Consent

Consent will only be required for direct marketing activities. Under the GDPR, it must be freely given, and an unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.

Data Breaches

Brokers should make sure they have the right procedures in place to detect, report and investigate a personal data breach. Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. Brokers will only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation,
financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. This must take place within 72 hours of becoming aware of the breach.

Brokers should put procedures in place to effectively detect, report and investigate a personal data
breach.

Financial Implications

Implementing the GDPR could result in some increased spending on training, appointment of specialist compliance staff and system changes which may have significant resource implications, especially for larger and more complex organisations.

Summary

- Increased Territorial Scope, the GDPR's will apply to all companies processing the personal data of data subjects residing in the European Union, regardless of the company's location. Previously, territorial applicability was ambiguous whereas GDPR makes it clear. Applies regardless of whether actual processing takes place in the EU or not.

- Penalties are another major change, under GDPR organisations can be fined up to 4% of annual global turnover or EUR 20,000,000 (whichever is greater). This applies to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

- Conditions for consent have been strengthened meaning companies will no longer be able to use long unintelligible terms and conditions full of legalese – request for consent must be in a clear, easily accessible form with the purpose fully explained. Must also be as easy to withdraw consent as it is to give it.

- Breach notification will become mandatory in all member states for certain types of breaches and must be reported within 72 hours of first having become aware of the breach.

- The data subject has an exclusive right to access personal data which is being processed about them and to ask if personal data concerning them is being processed.

- Privacy by design – calls for the inclusion of data protection from the onset of the designing of systems, rather than in addition. The ICO is not prescriptive on this, but it is up to Brokers to demonstrate the adequacy of their systems they have in place.

Conclusion

It is difficult to predict just how the new law will affect Brokers/Intermediaries with much of the full scope of the regulation yet to be agreed it may take many years to fully affect brokers in their day to day working.

In practice, the impact of the GDPR will vary from broker to broker depending on the size and complexity of the organisation, the true extent of the reforms and the actual amount of changes which will need to be implemented.

Brokers/Intermediaries must review training for all staff in preparation of the law coming into effect as the law has the potential to make a big impact on their work activities.
It will also be important for brokers to think practically about the data they hold and the journey that the data goes on from when it is collected, stored and shared with other parties. As it will now be important for organisations to be able to evidence where data has come from and who it has been shared with.

The final point that brokers need be aware of is that the consequences of failing to comply or breaching the new regulations are far more punitive that current arrangements. With maximum fines being enforced up to 4% of global turnover or up to EUR 20,000,000. Therefore, compliance is essential in order to protect their companies Balance Sheet from a large fine, but to also protect the companies and the industry as a whole's reputation.

Bibliography

1. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr
2. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
3. http://www.stride-group.co.uk/gdpr-what-insurance-brokers-need-to-know
4. https://view.publitas.com/biba/a-biba-brokers-guide-to-the-general-data-protection regulation/page/8-9
5. https://www.allianzebroker.co.uk/news-and-insight/news/general-data-protection-regulation.html
6. https://www.inforights.im/information-centre/data-protection/the-general-data- protection-regulation/gdpr-in-depth/rights/rectification/
7. https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf
8. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
9. https://www.marsh.com/uk/insights/research/what-the-new-eu-general-data-protection-regulation-gdpr-means-for-you.html

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