General Data Protection Regulation (GDPR) - UK

By Shaun Kelly BA(Hons) ACII FCILA FUEDI-ELAE MBCI, Crawford & Company and David Parker ACII Crawford & Company

CILA Synergy Committee

May 2018

General

This document provides guidance to members of the Chartered Institute of Loss Adjusters concerning the implications of the GDPR which is effective from 25 May 2018. The GDPR replaces the EU Data Protection Directive 1995 that was enabled in the UK as the Data Protection Act 1998. As a regulation it is directly applicable across all member states without the need for national implementing legislation. Organisations in the UK will be subject to the GDPR until the UK leaves the European Union in 2019 but the UK Government has made clear its continuing compliance with the GDPR would not be affected by Brexit and to this end has introduced the new UK Data Protection Bill, currently going through the UK legislative process. The new Bill will replace the Data Protection Act 1998 and is designed to not only apply the GDPR standards, but cover processing that does not fall within EU law and introduce other provisions to make the GDPR work better in the UK.

The GDPR applies to organisations processing the personal data of individuals (data subjects) in the European Union irrespective of their location. Personal data means any information relating to a natural person (living individual) who can be directly or indirectly identified in particular by reference

to this data or in conjunction with other data that might reasonably come into someone's possession (e.g. an identifier such as a policy or claim number). The GDPR applies to both automated personal data systems and to manual filing systems where personal data are accessible according to specific criteria such as individual claim files.

The principles under which personal data shall be processed are broadly the same as those under the existing legislation and it is the Controller that should be responsible for and able to demonstrate compliance with those principles. Compliance with the GDPR is an important issue as both individuals (i.e. members) and firms can be subject to a range of enforcement action for breaches of the GDPR. These include financial penalties which can be severe (up to €20m or 4% of the global revenue of a firm, whichever is the higher) as well as the associated damage to the reputation of the individual, the firm and the profession.

Loss Adjusters, acting on behalf of their clients, collect and process a wide variety of data involving private individuals whilst handling losses. The aim of the GDPR is the protection of privacy of individuals and members will correctly want to ensure that they control and process data legally and ethically. Members are reminded of the core principles of the Guide to Professional Conduct and in particular:

2.2 A member should behave ethically and with integrity in all professional and business relationships. Integrity implies not merely honesty but fair dealing, truthfulness and acting responsibly at all times. When communicating with any party, a member should do so in a way that is accurate, straightforward and understandable by that party.

As with any other matter of compliance, the law is simply the starting point, the basic essential element. As a member of this Institute you hold out to act in a manner in keeping with the wording and ethos of the Guide to Professional Conduct. In brief, if you need to question whether a behaviour is legal you should also question whether even if it were legal is it ethical, fair, true and responsible?

The following is taken direct from the Information Commissioner's Office website at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

a) *The GDPR applies to 'Controllers' **and** 'Processors'.*

b) *A Controller determines the purposes and means of processing personal data.*

c) *A Processor is responsible for processing personal data on behalf of a Controller.*

d) *If you are a Processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.*

e) *However, if you are a Controller, you are not relieved of your obligations where a Processor is involved – the GDPR places further obligations on you to ensure your contracts with Processors comply with the GDPR.*

f) *The GDPR applies to processing carried out by organisations (and their employees) operating within the EU. It also applies to organisations (and their employees) outside the EU that offer goods or services to individuals in the EU.*

g) *The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.*

The role of a loss adjuster

The distinction between a Data Controller and a Data Processor is fundamental to the concept of data protection compliance. Insurer clients are certainly Data Controllers. The role of a loss adjuster acting in that capacity or as a claims handler in a Third Party Administration agreement will usually be processing personal data as a data Processor, acting under the clients' direction and control. Even where the loss adjuster takes decisions in certain circumstances, for example whether to collect or disseminate other information as part of any investigation or whether to settle a claim, will be based upon criteria or instructions defined by the insurer. Generally loss adjusters or claims handlers will not have the latitude or discretion to decide to process data collected for purposes other than that set out in the contract or instruction from the client. Insurer clients very substantively regard loss adjusters as data Processors but in some very specific instances an insurer may regard loss adjusters as joint or independent data Controllers.

In circumstances where the loss adjuster processes data beyond the instructions from the insurer client there is a risk that the adjuster may stray into a controlling role. For example if the adjuster continues to hold data for longer than contract with the Insurer permits, generally following the limitation periods applying to first or third party claims. Other examples would be using data that had

not been obfuscated for general data analytical purposes or as part of test data for the development of a claims management application.

Deciding who is a Controller and who is a Processor may not always be clear cut and there may be scope for differences in interpretation and issues could possibly arise where independent legal advice must be sought. It would be impossible in this guidance document to articulate and respond to all the scenarios. Where the activity of a member is actually as a Data Controller they must ensure that the activity is represented in a Privacy Notice published to data subjects in accordance guidance published by the ICO at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/. That privacy notice must be published prior to gathering personal data.

The GDPR brings about a material change in the responsibilities of Data Processors which for the first time will have direct legal responsibilities placed upon them and will also be subject to enforcement action including the potential for substantial fines in the event of the breach. Under the GDPR (subject to some exemptions) Processors will be directly required to:

- keep records of processing activities
- appoint a data protection officer
- obtain consent from the data Controller before engaging a service provider (Sub-Processor) for processing
- tell the data Controller if there is a data breach
- put in place appropriate technical and organisational measures to safeguard personal data
- cooperate with the relevant supervisory authority (The Information Commissioner's Office in the UK)
- comply with the GDPR rules on cross-border transfers of data: and
- carry out data privacy impact assessments

In any event as detailed above you are required to act in a manner which meets the requirements of the CILA Guide to Professional Conduct.

How to be compliant

There must be a lawful basis for processing data. An Insurer as a Data Controller usually relies on contract with the data subject or the data subject's specific consent as a lawful basis for processing.

The loss adjuster as a Data Processor must only act on the documented instruction of the Controller in terms of processing the data. There must be a written contract in place between the Data Controller and the loss adjuster (their firm) as the Processor detailing the nature of the processing, the category of data subjects (e.g. their customers), the nature and purpose of the processing, the types of personal data to be processed and the subject matter and duration of the processing.

The loss adjuster must only process data necessary for the Controller's lawful purpose i.e. not gather, process and hold medical information or details of criminal convictions where such information is not necessary for the claim that they are handling or legitimate for the Insurer's underwriting purposes. Loss adjusters should only ever collect and process the minimum data necessary to perform their service.

Loss adjusters often involve other parties as a service provider on a claim. These may be an external expert, such as a forensic scientist or a supplier/contractor that provides claims fulfilment. Where such a third party is from a client's supplier panel they would be direct Processors of the client and so the client has the responsibility for their engagement under GDPR. However, a loss adjuster acting as a Processor under their own direction may be permitted with the consent of the client to engage their own service providers that involves that service provider receiving and processing personal data. In this situation the service provider would be a sub-Processor and the Loss Adjuster is obligated to flow down equivalent terms and conditions to that sub-Processors but would remain liable for the sub-Processors acts or omissions.

Importantly members must ensure that the data subject is informed if they envisage passing on a data subject's information to another party/organisation. The loss adjuster should as best practice remind the parties that they deal with that they act on behalf of the Insurer client and in handling the claim may pass on the parties details to other parties such as Insurers suppliers or the loss adjusters nominated suppliers.

Members must ensure that they exercise appropriate technical and organisational measures to protect data against unauthorised or unlawful processing and against accidental loss, destruction or damage. The level of security should be appropriate to the risks represented by the processing e.g. how sensitive and confidential the data is and the degree of harm that will occur to the data subject as a result of a breach. Technical measures involved the use of technology e.g. encryption of portable devices, anonymization of data while organisational measures include Policy and training.

Under the GDPR mandatory notification of data breaches has been introduced. The Data Controller is required to notify personal data breaches to the regulator (in certain circumstances reflecting guidance available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) without undue delay and where feasible not later than 72 hours of becoming aware of the breach. Set categories of information must be provided in the notification. It is important that in the event of a personal data breach members (as Data Processors) take prompt action to report such breaches to their clients (usually within 24 hours of becoming aware). The ICO indicate that failing to report a loss of data may well result in significantly more severe penalties than correct reporting of data losses.

Members should also be aware of the expanded data subject rights available to individuals that goes beyond Subject Access Requests (the ability to receive a copy of one's data held by a Controller) to a right to erasure of data and data portability between Controllers. Members should promptly liaise with the Insurer client if they are aware that a data subject is availing themselves of these rights so that they can manage a response.

Resources

Members must be aware of and follow the GDPR compliance policies issued by firms that they are engaged by. This will allow members to ensure that data they process is consistent with the law and does not result in breaches.

Firms' policies will not only include the legal basis for processing data but also refer to data retention periods and what to do in the event of the loss of data. Members should be clear that they are adhering to these policies.

The ICO website is a great resource for further understanding (ICO.org.uk) and the ICO have a helpline available to all to address your concerns.

Finally, this document reminded members of the need to adhere the Guide to Professional Conduct. You may also seek to view this issue from the position of the data subject. Again the ICO provide guidance to the public to review whether their data is being handled correctly this may be found at https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly .