Notices to Members

No.1 2018/2019 - Implementation of the EU General Data Protection Regulation 2016/679 – General Guidance to Members

IG Circular February 2018

Dear Sirs,

Introduction

Regulation (EU) 2016/679 containing the General Data Protection Regulation (the "GDPR" or "Regulations") will come into force on 25 May 2018 when it will have direct effect in the EU/EEA[1]. The Regulation, which is some 88 pages long, may be found on EU Standard Model Clauses

This general guidance intends only to provide a brief introduction to the GDPR, as relevant to the West of England Ship Owners Mutual Insurance Association (Luxembourg), hereinafter referred to as the Club, and its Members. The impact of the Regulation will most often be felt in claims relating to personal injury and illness or other cases involving data originating from natural persons, or individuals. Data originating from a legal entity that does not contain personal information, or information otherwise not related to natural persons is unaffected.

The broad intention of the Regulation is to replace Directive 95/46/EC and strengthen and harmonise EU/EEA procedures concerning the collection, storage, processing, access, use, transfer and erasure of personal data. By establishing responsibilities for "controllers" and "processors" of personal data, the Regulation aims to provide natural persons with the same level of legally enforceable rights throughout the EU/EEA, and a supervisory and enforcement framework to ensure compliance.

The aim of the GDPR is to protect natural persons in relation to the processing of data. The Regulation applies to those within the EU/EEA which may hold such data, but also to those outside the EU/EEA which may offer goods or services to natural persons within that area, or send personal data to organisations within the EU/EEA, or send personal data to recipients within the EU/EEA. Because the Club operates within the EU/EEA, the GDPR will apply to it. Similarly, the Regulation will apply to Members, and third-party service providers operating within the EU/EEA or offering goods or services to natural persons within that area, and to personal data held within the EU/EEA belonging to individuals who are outside the EU/EEA.

Penalties for infringement

The level of administrative fines under the new regime is substantially higher than under the old legislation. The amount of a fine will depend on a number of factors in each individual case, including, but not limited to, the nature and duration of the infringement, and any actions taken to mitigate damage suffered by the Data Subject. It is, however, worth noting that the penalties for infringements of the GDPR, in relation to certain provisions, can be up to €20 million or in the case of an undertaking, up to 4% of the worldwide annual turnover of the preceding financial year, whichever is higher.

Relevant definitions[2]

- **"Personal Data"** means any information relating to a Data Subject;
- **"Data Subject"** means an identified or identifiable living natural person or individual. This is someone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of the relevant data.
- **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated or manual means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Roles of the Club, Members, brokers, external service providers and claimants

The Club considers that it will be a controller for the purposes of the Regulations. The Club outsources day to day management to the West of England Insurance Services (Luxembourg) S.A., which will act as a joint controller. This will permit the Club to operate under the GDPR framework built by the West of England Insurance Services (Luxembourg) S.A. which will be able to perform administrative tasks that only a controller or joint controller are permitted to do. The West of England Insurance Services (Luxembourg) S.A. will also be able to represent the Club when dealing with the Data Regulator.

Further, where the GDPR applies, Members, brokers and external service providers such as club correspondents, surveyors, and experts, will generally be controllers, since they are each independently likely to determine the purpose and means of the processing of the relevant data. If a processor determines “the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing”[3].

This would be relevant only where the matter in issue, for example a personal injury or an illness claim, contains personal data. In that case, the relevant individual(s) bringing the claim would be the data subject, benefiting from the rights provided in the GDPR.

Some relevant requirements of the GDPR:

- Principles for processing personal data;
- Rights of the data subject;
- Responsibilities of the controller and processor;
- Duty to notify Data Protection Authorities;
- Appointment of Data Protection Officer; and
- Transfer of personal data to third countries.

Priciples for processing personal data[4]

The principles for processing personal data can be summarised as follows:

- *Lawfulness*[5] – personal data should be processed only when there is a legal basis for doing so, such as consent, by contract, or where there is a legal obligation, or where it is necessary in order to protect the vital interests of the data subject, or where it is for the legitimate interests of the controller.
- *Fairness* – those involved in processing personal data should provide the data subject with sufficient information about the processing and the data subject's rights.

- *Transparency* – information should be provided in a concise and readily understandable manner.
- *Purpose limitation* – personal data should only be collected and processed for specified, explicit and legitimate purposes and it should not be processed for reasons unconnected with these purposes.
- *Data minimisation* – personal data should be adequate, relevant and limited to what is necessary for the purposes for which it has been collected and processed.
- *Accuracy* - personal data should be accurate and up-to-date.
- *Storage limitation* – personal data should be kept in a form permitting identification of data subjects for no longer than is necessary.
- *Security* – using appropriate measures, personal data should be secured to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

Personal Data

Processing of personal data is prohibited unless specific conditions apply, such as express consent or where processing is a necessary consequence of the establishment, exercise or defence of legal claims, or wherever courts are acting in their judicial capacity[6]. It is recommended however that all Members and their associated named assureds, brokers, agents, etc. consider including suitable GDPR wording in contracts, employment contracts, collective bargaining agreements, ticket conditions, etc. to allow the processing of sensitive personal data on a permitted basis. This will be of particular importance when dealing with claims involving minors where more stringent GDPR conditions apply.

Specific, stricter requirements apply to sensitive personal data. This includes data such as race, ethnic background, religious and political affiliations, and health and medical information about a data subject.

Rights of the data subject[7]

Below is a summary of the rights which the data subject has, including the right to request information.

- *Transparency and information* – steps should be taken to provide the required information to the data subject, including details of the controller(s) and the purpose of processing the relevant personal data[8]. This includes advising the data subject of any third parties to whom the personal data will be disclosed.
- *Right of access* – the data subject has a right to require a confirmation of whether personal data is being processed, and for what purpose, and that there is a right to request access to it[9].
- *Right to rectify* – the data subject has a right to rectify inaccurate information[10].
- *Right to be forgotten* – the data subject has a right to request that his or her personal data is erased, without undue delay, if certain conditions apply[11].
- *Right to restrict processing* – the data subject has a right to obtain from the controller restriction of processing where, for example, the accuracy of the personal data is contested by the data subject.

Responsibilities of the controller, joint controller(s) and processor

The controller and joint controller

The controller and joint controller are required to implement appropriate measures for the processing of personal data in accordance with the Regulation[12]. This includes establishing and implementing a 'data protection policy' and other specific requirements, such as:

- *Only data necessary for the purpose* – procedures must ensure that only personal data necessary for the purpose is processed[13].
- *Processor* – procedures must ensure that the processor has implemented compliant measures.

The controller and joint controller are responsible for demonstrating compliance with the Regulation[14].

In the case of the Club, it is envisaged that it will be the controller, and the West of England Insurance Services (Luxembourg) S.A. will be a joint controller. Members and their assureds will be controllers of the personal data that they have received from their crew and claimants.

The processor

The processor must provide guarantees to the controller of appropriate technical and organisational measures so that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject[15]. A separate contract or agreement complying with specific requirements should be concluded between the controller and the processor.

Both controller and processor are responsible for the following:

- Record of processing – processing records should be maintained and these should be available for inspection by the supervisory authority[16].
- *Security of processing* – appropriate security measures should be established[17].

Duty to notify Supervisory Authority

The controller shall notify the appropriate Supervisory Authority of a personal data breach[18] in accordance with the GDPR where the rights and freedoms of the data subject have been affected. The processor is obliged to notify if it becomes aware of a breach of the GDPR[19].

Data Protection Officer

In certain circumstances, including where personal data is processed on a large scale[20], there is a duty to appoint a Data Protection Officer ("DPO")[21]. The DPO has specific responsibilities, including the monitoring of compliance with the Regulation, to report and to give internal advice.

Transfer of data to a third country

Unless there is a valid legal basis or permitted derogation under the GDPR for transferring data to a third country, in other words outside the EU/EEA, which may be the case where the transfer is necessary (such as in accordance with a legal obligation) to bring an insurance claim, for example a personal injury claim, then a transfer of data to a third country requires either the EU Commission to have decided that the relevant third country has established adequate levels of protection or that the controller or processor in the third country[22] has established or will establish appropriate levels of security[23].

In some circumstances, the use of the EU Standard Model Clauses may be appropriate: Read the EU Standard Model Clauses

What does the Regulation mean for the Club and its Members and what measures ought to be taken?

Some of the actions the Club has taken, or is in the process of taking, in response to the GDPR are as follows:

- A Data Protection Policy is being implemented;
- Internal written procedures and processes are being updated to include, for example, a regular review to ensure that unnecessary personal data is deleted;
- Standard privacy notices to data subjects giving details of rights under the GDPR will be issued when required[24]; and
- The security and integrity of IT and communication systems will be verified, in relation to both systems containing personal data and systems containing sensitive personal data.

Further impact on Members
Members operating within the EU/EEA area and those outside the EU/EEA offering goods or services to individuals in that area, or who hold personal data within the EU/EEA relating to individuals outside the EU/EEA, may need to undertake a similar exercise. The Club recommends that affected Members undertake a review with a focus on the following areas:

- Updating or adoption and implementation of a Data Protection Policy;
- Organisations handling data on a large-scale ought to consider the appointment of a DPO;
- Establish routines to ensure that data subjects receive appropriate information about processing of personal data and their rights;
- Unless there is another legal basis upon which to continue to store it, personal data which is no longer necessary should be deleted;
- Security should be enhanced for communications with third parties (including other P&I clubs) relevant to sensitive personal data as defined (e.g. health and medical data); and
- Additional checks should be established to ensure that personal data is transferred to third countries only when permitted (e.g. when there is a legal basis or a separate agreement exists).

This circular should not be construed as providing legal advice. Members should seek independent advice from a lawyer or their local Data Protection Authorities, when making changes in working routines with a view to ensuring compliance with the GDPR regulations.

Any questions or comments can be directed to Phillip Whitmore at phillip.whitmore@westpandi.com or on +44 (0)2077 166086.

All Clubs in the International Group have issued a similar circular.

Yours faithfully,

For: **West of England Insurance Services (Luxembourg) S.A.**
(As Managers)

T. Brevet
General Manager

---

[1] The EU/EEA means in this context The European Economic Area (EEA) which unites the EU Member States and the three EFTA States (Iceland, Liechtenstein, and Norway).
[2] From GDPR, Article 4.
[3] From GDPR, Article 28.
[4] GDPR, chapter II.
[5] GDPR, Article 6.
[6] GDPR, chapter II, articles 7 and 9.
[7] GDPR, chapter III.
[8] GDPR, chapter III, articles 12, 13 and 14.
[9] GDPR, chapter III, article 15.

[10] GDPR, chapter III, article 16.
[11] GDPR, chapter III, article 17.
[12] GDPR, chapter IV, article 24.
[13] GDPR, chapter IV, article 25.
[14] GDPR, Article 5.
[15] GDPR, Article 28.
[16] GDPR, chapter IV, article 30.
[17] GDPR, chapter IV, article 32.
[18] GDPR, Article 33
[19] The supervisory authority in [country] is [name of regulator].
[20] GDPR, chapter IV, article 37, 38 and 39.
[21] Contact details for the Data Protection Officer in [Club] can be found on [website].
[22] GDPR, chapter V.
[23] GDPR; chapter V, article 49.1.
[24] GDPR, Article 12.