CIRCULAR

The Standard for service and security

Standard Club

TO ALL MEMBERS

28 February 2018

Dear Sirs

Implementation of the EU General Data Protection Regulation 2016/679, general guidance to members

Introduction

Regulation (EU) 2016/679 containing the General Data Protection Regulation (the "**GDPR**" or "**Regulation**") will come into force on 25 May 2018 when it will have direct effect in the EU/EEA[1]. It will be incorporated into the law of the United Kingdom under the Data Protection Act 2018, which is expected to enter into force at the same time. The Regulation, which is some 88 pages long, may be found via the following link:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

This general guidance intends only to introduce the GDPR, as relevant to The Standard Club and its members. The impact of the Regulation will be felt, in particular, in claims relating to personal injury and illness or other cases involving data originating from natural persons, i.e. living individuals. Data that does not contain personal information, and information otherwise not related to natural persons is unaffected and falls outside the scope of the GDPR, unless such data can (in combination with other data) enable a natural person to be identified.

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.

[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).

The aim of the GDPR is to protect natural persons in relation to the processing of their personal data. The Regulation applies to those within the EU/EEA, which may hold or otherwise handle such personal data, but also to those outside the EU/EEA, which (i) process personal data in the context of the activities of a controller or processor established within the EU; (ii) offer goods or services to natural persons within the EU, or (iii) monitor the behaviour of natural persons to the extent such behaviour takes place within the EU. Because The Standard Club operates within the EU/EEA, the GDPR will apply to the club. 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 the EU, and to personal data processed within the EU/EEA relating to individuals who are outside the EU/EEA. The Regulation could also be applicable to members outside the EU/EEA who process data originating from EU/EEA natural persons by virtue of contractual obligations with EU/EEA companies.

Penalties for infringement

The level of administrative fines under the new regime is substantially higher than under the old legislation (Directive 95/46/EU and its implementing legislation - which, in the UK, is the Data Protection Act 1998). 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, i.e. an 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, conditions and means of the processing of the relevant data.

[2] From GDPR, Article 4.

- **"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 Standard Club, members, brokers, external service providers and claimants

The Standard Club considers that it will be a controller for the purposes of the Regulations. The club wholly outsources management to Charles Taylor & Co (Bermuda), who in turn delegates day-to-day administration to Charles Taylor & Co. Limited in London and other companies within the Charles Taylor group (the "managers") who will in most circumstances, act as a controller in common. This will permit the club to operate under the GDPR framework built by the managers and they will be able to perform administrative tasks that only a controller or joint controller are permitted to do. The managers will also be able to represent The Standard Club when dealing with the relevant supervisory authority.

Where the GDPR is applicable, whether a member, broker or external service provider, such as a club correspondent or surveyor, is acting as a controller or processor will depend upon whether they, in the particular circumstance are determining the purpose and means of the processing of the relevant personal data. 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.

For example, The Standard Club takes the view that a correspondent will usually be a processor. This is based on the assumption that: (i) the correspondent will at all times be processing personal data on behalf of the member and/or club; and, (ii) while they may have a degree of autonomy over how they process personal data to fulfil the requirements of the member and/or club, ultimately the direction over how such personal data will be used by the correspondent in the handling of a matter will be prescribed by the member and/or club. Moreover, even though there may not be a written contract in place between the member and the correspondent, the correspondent nonetheless has no authority to use the personal data for their own purposes and, in practice, would not be doing so. Correspondents are, however, capable of being a controller of personal data, for example where they are (i) processing the personal data for their own purposes and/or (ii) determining either jointly or in common with The Standard Club and/or a member, the manner and purposes of processing, and/or (iii) exercising a high degree of autonomy over the manner in which personal data are processed.

Some relevant requirements of the GDPR.

- Principles for processing personal data;
- Rights of the data subject;
- Responsibilities of the controller, joint controller(s), controllers in common and processor;
- Duty to notify the relevant data supervisory authority;
- Appointment of Data Protection Officer; and
- Transfer of personal data to third countries.

Principles for processing personal data[3]

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

- *Lawfulness*[4] – 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.

[3] GDPR, chapter II.
[4] GDPR, Article 6.

Sensitive personal data

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

Processing of sensitive personal data is prohibited unless specific conditions apply, such as explicit 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[5]. It is recommended however that all members and their associated named assureds, brokers, agents, etc. take steps to ensure that there are appropriate (GDPR-compliant) consents in place or alternative legal grounds for processing sensitive personal data. This will be of particular importance when dealing with claims involving minors where even more stringent GDPR conditions apply.

Rights of the data subject[6]

Below is a summary of many 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[7]. 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 obtain a confirmation of whether personal data is being processed, and for what purpose, and a right of access to it[8].

- *Right to rectify* – the data subject has a right to rectify inaccurate personal data[9].

- *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[10].

[5] GDPR, chapter II, articles 7 and 9.
[6] GDPR, chapter III.
[7] GDPR, chapter III, articles 12, 13 and 14.
[8] GDPR, chapter III, article 15.
[9] GDPR, chapter III, article 16.
[10] GDPR, chapter III, article 17.

- *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), controllers in common 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[11]. 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[12].

- *Processor* – procedures must ensure that the processor has implemented compliant measures.

The controller and joint controller are responsible for demonstrating compliance with the Regulation[13].

Controllers in common

The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

In the case of The Standard Club, it is envisaged that the club and the managers will in most circumstances act as controllers in common. 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[14]. A separate contract complying with specific requirements should be concluded between the controller and the processor.

[11] GDPR, chapter IV, article 24.
[12] GDPR, chapter IV, article 25.
[13] GDPR, Article 5.
[14] GDPR, Article 28.

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 relevant supervisory authority[15].

- *Security of processing* – appropriate security measures should be established and maintained[16].

Duty to notify the supervisory authority

The controller shall notify the appropriate supervisory authority of a personal data breach[17] 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[18].

Data Protection Officer

In certain circumstances, including where personal data is processed on a large scale[19], there is a duty to appoint a Data Protection Officer ("**DPO**"). 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 for transferring data to a third country, (in other words, a country outside the EU/EEA,) which may be the case where the transfer is necessary (such as in order to conclude or perform a contract in the interests of the data subject) 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[20] has established or will establish appropriate safeguards[21]. If adequate safeguards are required, the EU Standard Model Clauses may be used:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

[15] GDPR, chapter IV, article 30.
[16] GDPR, chapter IV, article 32.
[17] GDPR, Article 33.
[18] The supervisory authority in the United Kingdom is the Information Commissioner's Office
[19] GDPR, chapter IV, article 37, 38 and 39.
[20] GDPR, chapter V.
[21] GDPR; chapter V, articles 46 and 49.1.

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

Some of the measures the club has taken, or is in the process of taking, in anticipation of the Regulation coming into force in May are as follows:

- A Data Protection Policy has been established – implementation of the policy is anticipated in May 2018;
- The club's rules have been amended[22] to clarify that the conditions relating to the sharing and processing of personal data between, by and/or on behalf of the club and the member is contained in a separate data sharing agreement available on the club's website.
- A DPO has been appointed;
- Internal written procedures and processes are being updated to include, for example, a regular review to ensure unnecessary personal data is deleted;
- Standard privacy notices to data subjects giving details of rights under the GDPR will be issued when required[23]; and
- The security and integrity of IT and communication systems have been 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 and those outside the EU/EEA offering goods or services to individuals in that area, or who hold or otherwise process personal data within the EU/EEA relating to individuals outside the EU/EEA, or members outside the EU/EEA who process data originating from EU/EEA natural persons by virtue of contractual obligations with EU/EEA companies, 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;

[22] http://www.standard-club.com/media/2633623/21-december-2017-standard-europe-circular-rule-changes.pdf
[23] GDPR, Article 12.

- 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 that 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

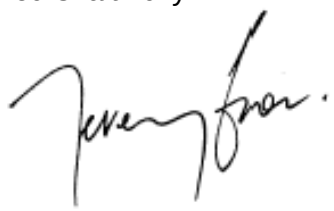
- Additional checks should be established to ensure that personal data is transferred to third countries only when permitted (e.g., when there is a legal basis or a separate agreement exists).

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

Any questions or comments can be directed to shahram.shayesteh@ctplc.com, Compliance Manager, in our London office.

All clubs in the International Group will be issuing a similar circular.

Yours faithfully



Jeremy Grose
Chief Executive
Charles Taylor & Co Limited

Direct Line: +44 20 3320 8835
E-mail: jeremy.grose@ctplc.com