BRITANNIA P&I
TRUSTED SINCE 1855

CIRCULAR

31 July 2018

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 the "Regulations") came into force on 25 May 2018 and has direct effect in the EU/EEA[1]. It has been incorporated into UK law under the Data Protection Act 2018. The EU Regulation, which is 88 pages long, may be found here: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

This general guidance, in conjunction with further information on the Britannia website, is intended to provide a brief introduction to the GDPR as it relates to Members' interaction with Britannia.

The Regulations will have greatest application to the handling of personal injury and illness claims or other claims that require a significant use of personal data. If the data does not contain personal information, or is information otherwise unrelated to natural persons (e.g. a company), it is unaffected.

The broad intention of the Regulations is to replace EU 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 Regulations aim 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 Regulations apply to parties within the EU/EEA which may hold such personal data, but also apply to those outside the EU/EEA which offer goods or services within the EU/EEA, or send personal data to organisations or other recipients within the EU/EEA.

Britannia is domiciled and operates within the EU/EEA and so GDPR applies to all personal data that is processed by us. The Regulations apply equally to Members and third-party service providers operating or offering goods and services within the EU/EEA and to personal data held within the EU/EEA belonging to individuals who are outside the EU/EEA.

[1] In this context, the EU/EEA means the European Economic Area (EEA) which means the EU Member States and the three EFTA States (Iceland, Liechtenstein and Norway).

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 Britannia, Members, brokers, external service providers and claimants

Britannia is a controller for the purposes of the Regulations. Britannia outsources its day to day management to Tindall Riley (Britannia) Ltd ("TRB"), who act as a joint controller. This permits Britannia to operate under the GDPR framework established by TRB and TRB will be able to perform administrative tasks that only a controller or joint controller is permitted to do. TRB will also be able to represent Britannia when dealing with Data Regulators.

Further, where the GDPR applies, Members, brokers and external service providers such as club correspondents, lawyers, 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].

The status as Controller or Processor is of primary significance where the matter in issue, for example a personal injury or an illness claim, contains personal data. In such a 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.

[2] From GDPR, Article 4.
[3] From GDPR, Article 28.

Principles 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 with the consent of the Data Subject, to fulfil a contract, 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 those 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.

[4] GDPR, chapter II.
[5] GDPR, Article 6.
[6] GDPR, chapter II, articles 7 and 9.

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 their 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 Regulations[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 Regulations[14].

Britannia and TRB act as joint controllers. Members and their assureds will be controllers of the personal data that they receive from other parties, such as their crew, agents or other third parties.

[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.

The processor

The processor must provide guarantees to the controller of appropriate technical and organisational measures so that processing will meet the requirements of the Regulations 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 its 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"). The DPO has specific responsibilities, including the monitoring of compliance with the Regulations, to report and to give internal advice. Dan Wilkinson has been appointed as Britannia's and TRB's DPO.

Transfer of data to a third country

GDPR creates a common set of expectations across the EU and so when considering the Security of personal data, transfer of data is permitted within the EU / EEA since receiving firms will be bound by the same regulation.

Transferring data outside of the EEA can be performed in three ways:

1. To a territory that the EU has determined offers adequate levels of Personal Data. This list is found at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu and so far recognizes Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (where the receiving entity is registered under the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with Japan and South Korea.
2. Where the agreement between the firm transferring the personal data and that receiving it provides safeguards that give adequate data protection. It is suggested that EU Standard Model Clauses may be appropriate and these can be found at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

[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.

3. Lastly, personal data can be transferred outside the EU or recognised territories where a derogation (relaxation of the rules for a specified purpose) exists. The most applicable derogations include where the transfer is:
    a. Made with the consent of the Data Subject;
    b. Necessary for the performance of a contract made in the interests of the Data Subject between the Controller and another person;
    c. Necessary for important reasons of public interest;
    d. Necessary for the establishment, exercise or defence of legal claims; and,
    e. Necessary to protect the vital interests of the data subject or other persons, where the Data Subject is physically or legally incapable of giving consent.

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

Britannia has taken the following actions in response to the GDPR:

- A Data Protection Policy has been updated and implemented;
- A DPO has been appointed;
- Internal written procedures and processes have also been 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[21]; 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 area and those outside the EU/EEA offering goods or services to individuals within the EU/EEA, or who hold personal data within the EU/EEA relating to individuals outside the EU/EEA, may need to undertake a similar exercise. Britannia 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 or destroyed;
- 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).

[21] GDPR, Article 12.

Penalties for infringement

Penalties for breaches of the GDPR are substantially higher than under the old legislation. The amount of a fine will depend on a number of factors in each individual case. These include, but are not limited to, the nature and duration of the infringement and any actions taken to mitigate damage suffered by the Data Subject. It is important to stress that the penalties for infringements of certain provisions of the GDPR can be the higher of up to €20 million or, in the case of a corporate entity, up to 4% of its worldwide annual turnover of the preceding financial year.

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 Dan Wilkinson: dwilkinson@triley.co.uk
.