BRITANNIA P&I
TRUSTED SINCE 1855

# CIRCULAR

**31 July 2018**

**Implementation of the General Data Protection Regulation ("GDPR" or "Regulations") in claims handling**

The purpose of this circular is to provide Members, correspondents and others with further guidance on how to reduce the risk of a breach and inform you of some changes we will be making in how we handle personal data.

People claims, such as those involving crew or passenger illness and injury, present the greatest challenge to Britannia in ensuring the adequate protection of personal data.

**Data minimisation and privacy by design**

Britannia is a controller of personal data for the purposes of the GDPR, and therefore responsible for demonstrating compliance with the Regulations. As a result, and in line with the key GDPR principles of data minimisation and privacy by design, Britannia wishes to:

- limit the amount of personal information that is routinely circulated;
- make greater use of existing technology to securely transfer personal data; and,
- anonymise personal data, where this is possible.

Email circulation lists continue to expand, which means it can be difficult to spot when someone who should not be included has inserted themselves into an email chain. In addition, attempted fraud by email is increasing, with communications received from impersonators of those involved in the industry. These imposters are usually seeking financial gain but responding to such a message could additionally lead to a data breach by Britannia.

In handling personal illness or injury files it is often necessary to exchange sensitive personal data with Members, correspondents and service providers around the world on an urgent basis. This makes understanding and implementing GDPR principles of particular importance.

Recognising that Members, brokers and external service providers such as correspondents, surveyors, and experts will generally be data controllers in their own right, we would like to offer readers some "best practice" guidance in the form of 10 tips for the treatment of personal data:

1. **Respect** - treat everyone's personal data with the same respect you would wish for your own.

2. **Minimise the transmission of personal data by email or recorded on paper** – the less personal data being created and circulated, the easier it is to protect. Only send information which is necessary for the handling of the claim.

3. **Cybersecurity** – ensure computer systems are secure and make use of security measures such as password protection and secure email servers when transferring attachments containing passports, medical reports, contracts of employment etc. We use enforced encryption or web portals to protect information.

4. **Anonymisation** – aim to use identifiers for individuals, like crewmember, broker, surveyor etc. instead of names and dates of birth. Other identifiers could be the ship name, the nature of the incident, or the port of disembarkation, with a reference number. This applies not just to the subject heading and body of an email but also, where possible, to any documents which support the claim. If there is no alternative to using a name, we would recommend that it is cited with as few other identifiers as possible. In the future we will

adopt this approach for our communications, including claim descriptions. Once these steps are put into practice, we hope that, except for those directly handling the claim, it will not be possible to identify the individual who is the subject matter of the claim.

5. **Start afresh** - if you cannot avoid identifying an individual, do so once and then start a new email so that the same personal data is not repeated in the email chain.

6. **Reply all?** - before using "reply all", check that it is appropriate that everyone in the circulation list should actually receive the email you are about to send.

7. **Use Official email addresses** – do not use unofficial, private, or any other non-secure email accounts.

8. **Clear and lock** - keep your desk clear and your computer screen locked when you are away from your desk. Dispose of hard copy data in a secure manner.

9. **Familiarise yourself with GDPR -** including how it applies to your business and the penalties for non-compliance.

10. **Communicate these guidelines** - to everyone in your organisation.

Implementing the above security measures minimises the risks arising from handling personal data that both Britannia and Members are exposed to and we ask that you consider implementing these and other measures appropriate to your organisation.

**Extra-territorial reach of the GDPR as it applies to crew engaged within and outside the EU/EEA[1]**

As referred to in the General GDPR circular, the Regulations apply to owners, charterers and/or their managers who have establishments within the EU/EEA where they are processing personal data on EU/EEA individuals who are within the EU/EEA. For example, where an owner has its management within Greece and provides Greek senior officers to its ships, the personal data of those individuals will fall within the scope of the Regulations.

Where the Regulations can have extra-territorial reach is if there is transfer of data from EU/EEA to outside EU/EEA, such as maybe the case in the recruitment of crewmembers where:

- the owner/manager is located in the EU/EEA but engages crew from outside the EU/EEA
- the owner/manager is located outside the EU/EEA but engages crew from the EU/EEA
- the owner/manager is located outside the EU/EEA and engages crew from outside the EU/EEA, but the voyage passes through the EU/EEA, which may be lead to the transfer of data transfer from the EU/EEA to outside EU/EEA.

Many Members use local manning agents for the recruitment of crew outside of the EU/EEA, for example from the Philippines, India and the Ukraine. However, as the crew are engaged by an owner/manager with an establishment in the EU/EEA, the processing of their personal data will also fall within the scope of the Regulations, despite the crew themselves not being EU/EEA nationals.

[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).

Similarly, where an owner/manager is located outside the EU/EEA but engages crew from EU/EEA countries, as they will be processing personal data on EU/EEA individuals, that processing will also fall within the scope of the GDPR.

**Owners' privacy responsibilities**

In respect of crew illness and injury claims, Britannia will often be the owners' employers' liability insurers and in such cases, it will be necessary for the owner / manager to provide the crew with notice that their personal data may be shared with its insurers and other third parties.

We expect that for the majority of our Members, their crew contracts and collective bargaining agreements (CBAs) will either not contain data protection clauses/notices or they will need updating. We therefore ask Members to ensure that they provide their crew with the necessary notice.

In addition to any wider privacy notice (also known as an information notice or fair processing notice) you may have developed, we suggest that Members consider including in the notice the following provisions dealing with injury and illness claims:

- **What information is being processed?** - personal and financial information, as well as some sensitive data regarding the individual crew member's identity, health, illness and injuries.

- **Why is it being processed?** - to assist with medical treatment and insurance claims.

- **On what legal basis is it being processed? -** to protect vital interests of the individual, perform the employment contract, to respond to or defend any claim, to comply with legal or statutory obligations including the provision of insurance.

- **Who it may be transferred to?** - insurance companies, insurance brokers, health facilities and entities, either in or outside the EU/EEA, involved in the management of a claim and/or the treatment, travel and repatriation of a crew member.

- **How long will it be kept for?** - consideration should be given to the length of employment, limitation periods and other relevant factors; but the principle is to keep the personal data for as short a period as possible.

This is not an exhaustive list to ensure compliance with GDPR, but it should allow Members to provide claims information to Britannia in a lawful manner.

In addition, local and specific legal advice should also be obtained.

For other steps that we recommend to our Members, please refer to the "Further impact on Members" section in our other circular dated 31 July 2018.