Notices to Members

No. 6. 2018/2019 - Implementation of GDPR principles in claims handling

IG Circular June 2018

Dear Sirs

Implementation of GDPR principles in claims handling

The General Data Protection Regulation ("GDPR") provides for significant penalties in the event of a data breach. The purpose of this circular is to provide Members, correspondents and others with further guidance on how to try and reduce the risk of a breach and advise 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 the Club in ensuring the adequate protection of personal data.

Data minimisation and privacy by design

As mentioned in our previous circular, the Club is a controller for the purposes of the GDPR, and thus responsible for demonstrating compliance with the Regulation. As a result and in line with the key GDPR principles of data minimisation and privacy by design, the Club wishes to

- start limiting the amount of personal information in circulation,
- make greater use of existing technology to transfer personal data more securely and
- where possible, anonymise the data that is exchanged.

E-mail 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 e-mail 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 lead to a data breach by the Club as well.

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. Implementing GDPR principles is particularly important.

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 generation of personal data by email and 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 intend to use enforced encryption or web portals to protect information.

4. **Anonymisation** – aim to use identifiers for individuals, like crew member, broker, surveyor etc. instead of names and dates of birth. Other identifiers could be the vessel 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 e-mail but also, where possible, to any documents which support the claim. If there is no alternative to using an individual's name, we recommend that it is cited with as few other identifiers as possible. We also intend to adopt this approach for claim descriptions. If these steps are put into practice, we hope that, except for those directly handling the claim, it will not be possible to identify 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 e-mail 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.

Since the Club recognises that Members, brokers and external service providers such as Club correspondents, surveyors, and experts will generally be data controllers, as will be the Club, implementing the above security measures minimises the risks arising from handling personal data that both the Club 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

The Regulation applies to Shipowners 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 a Shipowner has its management within [Greece] and provides [Greek] senior officers to its ships, the personal data of those individuals will fall squarely within the scope of the Regulation.

Where the Regulation can have extra-territorial reach is if there is transfer of data from EU/EEA to outside EU/EEA, such as in the following cases:

the recruitment of crew members where

- the Shipowner/Manager is located in the EU/EEA but engages crew members from outside the EU/EEA
- the Shipowner/Manager is located outside the EU/EEA but engages crew members from the EU/EEA
- the Shipowner/Manager is located outside the EU/EEA and engages crew members 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.

For many of our Members, local manning agents are used for the recruitment of crew members 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 Regulation, despite the crew members themselves not being EU/EEA nationals.

In addition, where a Shipowner/Manager is located outside the EU/EEA but engages crew members 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 Regulation.

Shipowners' Privacy Responsibilities

In respect of crew illness and injury claims, the Clubs will often be the Shipowners' employers' liability insurers and in such cases it will be necessary for the Shipowner/Manager to provide the crew members 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 would therefore ask Members to ensure that they provide their crew members 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 sensitive data regarding the crew member's identity, health, illness and injuries. Financial information.
- 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 and to respond to or defend any claim, to comply with legal or statutory obligations for example, to provide 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.

This is not an exhaustive list to ensure compliance with GDPR, but should allow Members to provide claims information to the Club.

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

For other steps which the Club recommends Members should take, please refer to the *"Further impact on Members"* section in our previous circular.

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