

GDPR bulletin

April 2018

**The Standard
for service and security**



**Standard
Club**

Introduction

The European General Data Protection Regulation (GDPR) comes into force in the EU/EEA on 25 May 2018. This bulletin looks at the potential implications and issues to consider.



James Bean
Managing Director, Standard Europe
T +44 20 3320 8811
E james.bean@ctplc.com

When the board of The Standard Club met in Paris in January of this year, see the full report on [page 10](#), one of the hot topics for discussion was the European General Data Protection Regulation (GDPR), which comes into force in the EU/EEA on 25 May 2018. This new regulation is going to give the data protection rules across Europe their biggest overhaul in 20 years, significantly changing how businesses collect, store, process, access, use and transfer personal data. The GDPR 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. As well as putting new obligations on companies and organisations that are collecting personal data, the GDPR also gives individuals a lot more power to access the information that is held on them to and get their data erased in some circumstances. Failure to comply with the new regulations could result in significant fines.

Application

The GDPR applies to those within the EU/EEA that may hold or otherwise handle personal data, but also potentially to those outside the EU/EEA. Because The Standard Club operates within the EU/EEA, the GDPR will apply to the club. Similarly, the GDPR will apply to members, and third-party service providers operating within the EU/EEA or offering goods or services to identifiable living natural persons within the EU, and to personal data processed within the EU/EEA relating to individuals who are outside the EU/EEA. The GDPR 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.

In this edition

3	Data controllers and processors
6	GDPR – Roadmap to compliance
8	The GDPR and the club: what next?
9	Club cover
10	Board meeting
11	Office move

The table below considers a number of P&I-type scenarios where the GDPR should apply.

Scenario	Should GDPR apply?	Justification
<ul style="list-style-type: none"> • EU nationality crew member • EU flag state • EU based correspondent • EU regulated and domiciled member 	√	<p>The GDPR has a broad territorial scope.</p> <p>Pursuant to Article 3 of the GDPR:</p> <p><i>it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not.</i></p>
<ul style="list-style-type: none"> • Non-EU nationality crew member • EU flag state • EU based correspondent • EU regulated and domiciled member 	√	
<ul style="list-style-type: none"> • Non-EU nationality crew member • Non-EU flag state • EU based correspondent • EU regulated and domiciled member 	√	
<ul style="list-style-type: none"> • Non-EU nationality crew member • Non-EU flag state • Non-EU based correspondent • EU regulated and domiciled member 	√	
<ul style="list-style-type: none"> • Non-EU nationality crew member • Non-EU flag state • Non-EU based correspondent • Non-EU regulated and domiciled member 	X	No link with the European Union and therefore the GDPR does not apply.

Impact

It is clear that, when implemented, the GDPR will have a significant impact not only upon the club, but also upon a large proportion of the membership and service providers – in particular, in claims relating to personal injury and illness or other cases involving data originating from natural persons, ie living individuals.

Information

A few weeks ago, all the clubs in the International Group issued a similar [circular](#) providing general guidance to members on the implementation of the GDPR.

For this bulletin, we have teamed up with leading international law firm Reed Smith to take a closer look at:

- 1 the concept of data controllers and processors, and what this means in the context of P&I**
- 2 six pressing issues that should be on members' radar between now and 25 May**
- 3 the GDPR and the club: what next?**
- 4 The impact on club cover**

Data controllers and processors

The GDPR establishes responsibilities for 'controllers' and 'processors' of personal data. A good understanding of these concepts and their interplay is therefore of fundamental importance to ensure compliance. This article intends to explore potential data controller and processor scenarios in the P&I context.



Anna Kalogianni
Claims Executive,
Mediterranean and Middle East
T +44 20 7522 6464
E anna.kalogianni@ctplc.com

The broad intention of the GDPR is to 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 GDPR 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 concepts of data controller and processor therefore play a pivotal role in the application of the GDPR. The precise legal status of any third party – as controller or processor – will depend entirely on the factual circumstances relating to the processing of personal data. A good understanding of these concepts and their interplay is therefore of fundamental importance to ensure compliance.

This article intends to explore potential data controller and processor scenarios in the P&I context. However, before doing so, it is important to consider the definition of controller and processor.

Definition of controller and processor Article 4 of the GDPR states that:

'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 personal data.

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Effectively this means that the controller determines the purposes, conditions and means of processing personal data, whilst the processor is any person or entity other than an employee of the controller who processes personal data on behalf of the controller.

Joint controllers and controllers in common

However, there are a couple of different permutations of definition of controller. Article 26 of the GDPR states that:

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

Although not expressly defined in the GDPR or the repealing Directive 95/46/EC, the concept of 'controllers in common' is also recognised. In particular, the ICO [guidance for Directive 95/46/EC](#), which although not extended to the GDPR yet (but is unlikely to materially change), provides that:

In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

The legal status as controller or processor

The test is fact specific and depends on the context, the degree of control, the precise role and the parameters that have been set.

The following table explores potential data controller and processor scenarios in the P&I context.

Parties	Legal status	Source	Comments
Member and club	Controllers in common	ICO Guidance for Directive 95/46/EC	<ul style="list-style-type: none"> When two or more persons share a pool of personal data that they process independently of each other, as opposed to joint controllers who act together to decide the purpose and manner of any data processing. The view is that clubs are data controllers in their own right and use the data they hold for their own purposes.
Club and manager	Joint controllers	Article 26 of the GDPR	<ul style="list-style-type: none"> The club wholly outsources management to Charles Taylor & Co (Bermuda), which in turn delegates day-to-day administration to Charles Taylor & Co. Limited in London and other companies within the Charles Taylor group (the managers) which 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.
Club/member and third-party/ outsourced professionals, such as listed and non-listed correspondents, surveyors, experts, medical assistance companies, manning agents, lawyers, brokers, other clubs, etc	Controller and processor	Article 4 (7) and (8) of the GDPR	<ul style="list-style-type: none"> A controller is free to set the authority limits to a processor and permit the processor to operate autonomously within those authority limits without the processor necessarily being deemed a controller.
Club correspondent and third party suppliers	Processor and processor	Article 4 (8) of the GDPR	<ul style="list-style-type: none"> 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. However, the less control the clubs exercise over correspondents and the manner in which such correspondents process personal data on their behalf, the more likely it is that such correspondents may be deemed controllers in their own right. A potential scenario where a correspondent may be identified as controller is when the correspondent operates in the form of a group entity/agent which further internally delegates the day-to-day data handling to its staff.

“The concepts of data controller and processor play a pivotal role in the application of the GDPR. It is therefore important that members, correspondents and service providers have a good understanding and knowledge of these concepts”

Responsibilities and duties of the controller, joint controller 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 GDPR. This includes establishing and implementing a data protection policy and other specific requirements, such as procedures which must ensure that:

- only personal data necessary for the purpose is processed
- the processor has implemented compliant measures.

The controller and joint controller are responsible for demonstrating compliance with the GDPR.

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 GDPR and ensure the protection of the rights of the data subject. A separate contract complying with specific requirements should be concluded between the controller and the processor.

Both controller and processor are responsible for ensuring that they have:

- processes to ensure that records are maintained and available for inspection by the relevant supervisory authority
- established and maintained appropriate security measures.

Duty to notify the supervisory authority

The controller shall notify the appropriate supervisory authority of a personal data breach 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.

Conclusion

As can be seen from the above, the concepts of data controller and processor play a pivotal role in the application of the GDPR. It is therefore important that members, correspondents and service providers have a good understanding and knowledge of these concepts. We will be writing to the club's correspondents to further explain our expectations of them.



GDPR – Roadmap to compliance

This article highlights six pressing issues which should be on members' radar before the GDPR becomes effective.



Philip Thomas
Partner, Reed Smith
T +44 20 3116 3526
E pthomas@reedsmith.com



Sally-Ann Underhill
Partner, Reed Smith
T +44 20 3116 3617
E sunderhill@reedsmith.com

Introduction

As members are no doubt aware, the General Data Protection Regulation (the GDPR) will come into effect imminently. 25 May 2018 marks the end of a two-year transition period and the beginning of the biggest shake-up of EU data protection laws in over 20 years.

For members located in the UK, Brexit will not affect the applicability of the GDPR, since (in the short term) the GDPR will come into effect before the UK is set to leave the EU. The UK will also be bound by the GDPR following Brexit as the Data Protection Bill (currently in draft form) will transpose the GDPR into UK national laws. The GDPR is directly applicable in all EU jurisdictions and (as a result of its extra-territorial provisions) will apply to organisations in non-EU jurisdictions where specific criteria are met – in particular, where the organisation is: (i) offering goods or services to individuals in the EU; or (ii) monitoring the behaviour of individuals within the EU, to the extent that such behaviour occurs in the EU; or (iii) processing personal data in the context of the activities of an EU establishment (regardless of where the processing takes place).

The GDPR will present significant challenges for members operating in all sectors, including the shipping, transport, logistics and related sectors. Under the new regime, maximum fines for non-compliance will be 4% of global annual turnover, or €20 million, whichever is higher. With national data protection authorities across the EU promising to ramp up enforcement efforts, the financial consequences of failing to comply are very real, not to mention the potential reputational damage to businesses which could flow from regulatory action.

With just six weeks to go before the GDPR becomes effective, we highlight six pressing issues that should be on your radar between now and 25 May.

Data processing inventory

As well as it being a specific requirement under the GDPR to maintain a record of processing activities, creating an inventory of personal data that you process is a key first step in your compliance programme. Only once you are clear on what personal data you hold and where you hold it, will you be able to identify particular areas of compliance risk and take effective steps towards fulfilling your other obligations under the GDPR. If your personal data inventory has not yet been finalised, we recommend prioritising this in good time before the GDPR comes into effect.

“In the shipping, transport and logistics sectors, supplier relationships are likely to be more complex and interdependent than in many other sectors, and may involve the service provider acting in one or both capacities, depending on the context”

Data Protection Officer

Not every business will need a Data Protection Officer, and some which are not required to have one by law may still choose to appoint one. It is essential that, if you have not already done so, you complete your assessment of whether you are required to appoint a DPO. If a DPO is required, you must secure their appointment and ensure that they meet the minimum GDPR requirements before the 25 May deadline.

Supplier agreements

Vendor agreements should be reviewed to ensure that they align with the new requirements of the GDPR. Specifically, the GDPR requires such agreements to include minimum legal provisions. As part of that review, it is prudent to consider whether the service provider could be viewed as a ‘co-controller’ of personal data as opposed to a ‘processor’, as the answer will impact on the changes you propose to the agreement. In the shipping, transport and logistics sectors, supplier relationships are likely to be more complex and interdependent than in many other sectors, and may involve the service provider acting in one or both capacities, depending on the context. If you are yet to begin this exercise, we recommend prioritising the service providers who hold the most sensitive categories, or highest volumes, of personal data. Then, devise a compliance plan to bring those contract variations into effect.

Policies

Whilst most businesses will doubtless have pre-existing policies around data protection, it is necessary to check whether they need to be refreshed so they are GDPR compliant. It will almost certainly be the case that existing policies will need some tweaking and/or that new policies will need to be prepared to meet the standard required under the GDPR. For example, the GDPR requires data controllers to notify data subjects within 72 hours of becoming aware of a data breach, meaning that a clear data breach response policy is essential. Other policies that may be relevant include those that address individual rights (discussed below) and privacy, by default and by design.

Individual rights

The GDPR reinforces many of the existing rights that individuals already have under the existing EU data protection framework (for example, the right to access personal data), but it also introduces a raft of new or enhanced rights. For example, individuals on whom you hold personal data can, under certain circumstances, request the erasure or rectification of their personal data, its transfer in a portable format to a successor organisation or to the individuals themselves, as well as a right to object to their personal data being processed on certain grounds. With a one-month deadline to deal with all such requests, it is vital to ensure that defined policies and processes are in place to address how to handle them.

Data retention

The GDPR retains the principle that personal data should not be held longer than necessary, in relation to the purpose for which such data is processed. This applies not only to new data that is collected, but means that any existing data that is held, and that it is not necessary to hold to fulfil the relevant processing purposes, will be held in breach of the GDPR from 25 May 2018. As with all requirements of the GDPR, it applies to all personal data, whether this is held electronically or in paper files. This principle has been amplified by a right of erasure (also known as a ‘right to be forgotten’), which places a positive burden on organisations to manage proactively the duration for which personal data is kept.

Your data processing inventory should highlight those areas in which personal data is held and assist you in determining what is required for long-term retention. Holding personal data indefinitely in case it may be relevant in the future is not permitted, except in the most exceptional circumstances.



For those who require further support in getting up to speed with the GDPR and meeting the 25 May deadline, please contact either Philip Thomas or Sally-Ann Underhill at Reed Smith on their contact details above.

The GDPR and the club: what next?

The club has been putting measures in place to ensure compliance with the GDPR in advance of the 25 May deadline. This article outlines some of the key activities.



Shahram Shayesteh
Compliance Manager
T +44 20 3889 8208
E shahram.shayesteh@ctplc.com

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

- A data protection policy has been drafted – implementation of the policy is anticipated in May 2018.
 - The **club's rules** have been amended 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 are contained in a separate data sharing agreement available on the club's website.
 - A data protection officer will be appointed.
 - 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 their rights under the GDPR will be issued when required.
- The security and integrity of IT and communication systems containing personal data and containing sensitive personal data have been verified.
 - We are reviewing whether we need to email all our contacts to confirm the accuracy of contact details, whilst obtaining the necessary GDPR-compliant consent to hold and process their personal data.
 - We will be asking members from certain jurisdictions to opt in to receive marketing emails – this does not include Annual Reports, Rule books or Circulars.

The above list is not exhaustive and is only intended to illustrate the range of measures that members should expect their club to be taking.

Club cover

Whilst there is no express GDPR exclusion in the club's rules, it is unclear how a fine for a potential data breach could result in a P&I liability. This article outlines how P&I cover would respond.



Sam Kendall-Marsden
Legal Director

T +44 20 3320 8876

E sam.kendall-marsden@ctplc.com

In so far as a member did seek reimbursement from the club for such a fine, it would be discretionary under rule 3.16.4. This rule provides for a two-stage test:

1. Whether there is to be any recovery at all.

There is only recovery 'to the extent that the member has satisfied the board that he took all such steps as appear to the board to be reasonable to avoid the event giving rise to the fine'. The burden is upon the member to demonstrate this.

2. The amount of any recovery.

The amount of any such recovery is at the discretion of the board.

It is therefore important that members carefully consider the implications of the GDPR implementation and the measures that should be put in place to ensure compliance.



[P&I and Defence Rules and Correspondents 2018/19](#)



[Offshore P&I Rules and Correspondents 2018/19](#)



[Fixed Premium Rules and Correspondents 2018/19](#)



[London Class P&I and Defence Rules and Correspondents 2018/19](#)



[War Risks Class Rules 2018/19](#)



[Singapore War Risks Mutual Class Rules 2018/19](#)

Board meeting

The club board, and the boards of its principal subsidiaries, met in Paris on 30 January 2017. The club's class general meetings were held on the same day. On the previous day, meetings of the board's three committees – Audit and Risk, Strategy, and Nomination and Governance – took place, as well as a meeting of the club's asset allocation working group.



Jeremy Grose
Chief Executive
T +44 20 3320 8835
E jeremy.grose@ctplc.com

Board members

Four new directors were welcomed to the board of The Standard Club: Ronald Forest of Matson Navigation, Allister Paterson of CSL Group, Ken Soerensen of Algoma Central and Dr Chen-Huei Yeh of Kuang Ming Shipping. The board took the opportunity to thank Marianne Sørensen, formerly with Maersk, who retired from the board at the end of the meeting.

Renewal

The board received an update on the club's renewal, which has since successfully been concluded according to the approach agreed by the board and announced to members in October 2017. Namely, no general increase was applied to the 2018/19 policy year to any class of P&I (mutual, charterers or offshore) or defence premium, and for the second consecutive year, 5% of the mutual call is being returned to members for the 2017/18 policy year. This is in line with the board's aim, as a member-owned mutual, to keep premiums at the lowest sustainable level, balancing the need to support members with the need to maintain the club's financial strength.

Financial position

The board reviewed the financial position of the club, the 2017/18 financial year performance and the financial plan for future years. Full details of the club's financial position will be set out in the annual report and accounts, which will be published later this year.

Despite the challenging market conditions, the club's investments delivered a strong result for the period from 20 February 2017 to 20 February 2018 across all asset classes.

The board agreed that there would be no further calls on any policy year for all classes. Release calls are being maintained at their current level, which is low relative to other clubs, reflecting the board's confidence in the club's financial position and its appeal to members.

Club strategy

The board and its strategy committee reviewed the club's updated strategy and business plan, which reflect the strategy committee's discussion held in October 2017 on the club's strategic position and direction. The club's four strategic objectives – to offer a broad range of P&I insurance and other marine and energy covers that represent excellent and sustainable value; to be recognised as providing excellent service by solving members' problems; to maintain first-class financial security; and to achieve selective growth, consistent with the other objectives – remain unchanged. Club growth during the year from both existing and new members remains strong. This resulted in an increase in tonnage by the February renewal, which was higher than the world fleet growth for the same period. This strong growth outside the renewal season is a signal that members value the club's professional, personal service and financial security.

Brexit

During 2017, in response to the UK's decision to exit the European Union, the club announced its intention to make an application to the Central Bank of Ireland for approval of a new subsidiary. The board was updated on the ongoing preparation for the possibility that UK based insurers will not have authorisation to underwrite in the EU after March 2019. In view of this, around 40% of the club's business will need to be insured in this new subsidiary with effect from 20 February 2019. The board was pleased to note that the club's Brexit plans were on track, and that the managers were confident of having all the necessary regulatory approvals in place with plenty of time to spare, regardless of the outcome of negotiations between the UK and the EU for a transition arrangement.

The Standard Syndicate (Syndicate 1884)

The directors received an update from The Standard Syndicate's active underwriter and managing director. Whilst the syndicate's performance in the first three years of operation has been behind plan, the directors were pleased to note that affirmative actions taken to improve the syndicate's performance, including recruitment to strengthen both underwriting and operational capabilities, and further diversification of the portfolio, is starting to deliver measurable results with the syndicate's business plan for 2018 targeting profitable underwriting.

Next meeting

The board will next meet on 12 May in Rome.

Office move

After more than 8 years at their current location, the managers' London agents, Charles Taylor & Co Ltd, are moving to new CT plc headquarters in the heart of the city.

From 16 April, following the sale of Standard House by the club, the managers will be temporarily based at 131 Finsbury Pavement, London, EC2A 1NT.

On 2 July, all your usual London contacts will move to a new permanent address at:

The Minster Building
21 Mincing Lane
London
EC3R 7AG.

All telephone numbers and other contact details will be unaffected by these moves. However, The Standard Club's registered office address will be updated in April to the new permanent address at The Minster Building. We are working to reflect this change throughout our correspondence and documentation, and will issue a circular regarding our updated invoice details.

If you have any queries regarding the move, please get in touch with your usual club contact.

The Standard Club issues a variety of publications and web alerts on topical issues and club updates. Keep up to date by visiting the news section on our website www.standard-club.com

 **@StandardPandi**
 **The Standard P&I Club**

This GDPR Bulletin is published on behalf of The Standard Club Ltd by the managers' London agents: **Charles Taylor & Co. Limited**. Registered in England No. 02561548 Authorised and regulated by the Financial Conduct Authority FRN 785106.
Registered address:
Standard House, 12–13 Essex Street, London, WC2R 3AA

The information and commentary herein are not intended to amount to legal or technical advice to any person in general or about a specific case. Every effort is made to make them accurate and up to date. However, no responsibility is assumed for their accuracy nor for the views or opinions expressed, nor for any consequence of or reliance on them. You are advised to seek specific legal or technical advice from your usual advisers about any specific matter.

Telephone: +44 20 3320 8888
Emergency mobile: +44 7932 113573
E: pandi.london@ctplc.com
Website: www.standard-club.com

The Standard Club Ltd is regulated by the Bermuda Monetary Authority. The Standard Club Ltd is the holding company of the Standard Club Europe Ltd and the Standard Club Asia Ltd. The Standard Club Europe Ltd is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. The Standard Club Asia Ltd is regulated by the Monetary Authority of Singapore.

**Charles
Taylor**