

FAQS: GENERAL DATA PROTECTION REGULATION (GDPR)

JANUARY 2018

SPECIAL THANKS TO HILL DICKINSON, MAZARS AND PPT LEGAL FOR THEIR CONTRIBUTIONS TO THE BELOW FAQS.

GENERAL

1. WHEN DOES GDPR ENTER INTO FORCE?

25 May 2018.

2. WHAT CONSTITUTES A BREACH OF THE GDPR? CAN YOU PROVIDE EXAMPLES?

Administrative fines up to €20,000,000 or up to 4% of global turnover, whichever is higher for breaches of, for example:

- the basic principles for processing, including conditions for consent (Articles 5, 6, 7 and 9);
- data subjects' rights (Articles 12-22);
- international transfers (Articles 44-49);

Other infringements are subject to administrative fines up to €10,000,000 or up to 2% of global, whichever is higher for breaches of, for example:

- to implement technical and organisational measures to ensure data protection by design and default (Article 25);
- on controllers and processors not established in the EU to designate representatives (Article 27);
- on controllers in relation to the engagement of processors (Article 28);
- to maintain written records (Article 30);
- on controllers and processors to co-operate with supervisory authorities (Article 31);
- to implement technical and organisational measures (Article 32);
- to report breaches when required by the GDPR to do so (Articles 33-34);
- in relation to the conduct of privacy impact assessment (Articles 35-36);
- in relation to the appointment of Data Protection Officers (Articles 37-39);

Any violation of a GDPR obligation may constitute a breach. Indicatively, a breach could be: not implementing adequate security measures, not discharging Data Controller's obligations, violating or not allowing the exercise of rights vested with data subjects, not fulfilling the requirements for transferring data outside the EU, not abiding by the principles and rules for lawful processing of personal data, etc.

3. WHAT PROCESSES HAVE NORTH PUT IN PLACE FOR COMPLIANCE?

As we are established in the UK we will be reviewing our policies and procedures when final legislation and guidance is issued by the UK government and data protection regulator at the end of the year. We will be making sure policies, procedures,

documents and processes such as our data protection policy, data breach procedures, document retention procedures and privacy notices meet these requirements.

4. WILL INTERNATIONAL GROUP CLUBS' APPROACH TO THE GDPR BE CONSISTENT?

There may be some differences between approaches due to differences in clubs' operating models. For example, the relevant regulatory authority for many clubs will be the UK's Information Commissioner but other clubs are established in other countries in or outside of the EU. Clubs will take a consistent approach as far as possible.

5. WHAT CAN A COMPANY DO WHEN THEY HAVE NO IDEA WHERE TO START? IS IT POSSIBLE TO GET AN 'OFF THE SHELF' COMPLIANCE PLAN / POLICY?

Off the shelf policies are not available simply because it is important to tailor the plan/policy to the business. There are however a number of resources explaining how companies can get started. If you have any questions you can get in touch with your usual contact at the Club.

6. IS IT RECOMMENDED TO HAVE AN IN HOUSE DATA PROTECTION OFFICER OR AN INDEPENDENT ONE? COULD YOU SUGGEST SOME PROS AND CONS OF EACH?

The first question is whether a DPO is required.

Article 37 states:

1. The controller and the processor shall designate a data protection officer in any case where:
 - (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
- 2...
- 3...
- 4...
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

> Continued Overleaf

FAQS: GENERAL DATA PROTECTION REGULATION (GDPR)

JANUARY 2018

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7...

The question then is what constitutes, “*processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.*”

Guidelines on this can be found at, (although the definitions are far from satisfactory):

[Guidelines on Data Protection Officers \('DPOs'\), wp243rev.01_en](#)

It is difficult to give advice on whether to do this by way of in house or service contract. Much will depend upon an organisation's resources and whether the DPO can be used for other duties and will most likely be a commercial decision based on cost and convenience.

7. IS THERE A LIMIT TO THE SIZE OF A COMPANY THAT GDPR APPLIES TO? FOR EXAMPLE, COMPANIES EMPLOYING LESS THAN 250 PEOPLE?

The GDPR applies to all companies, including those with less than 250 employees (SMEs). However, SMEs are not required to maintain the record of processing referred to under Article 30 unless the processing is large scale or involves special category or criminal records data.

Note that the GDPR allows individual EU member states to consider whether they wish to amend the GDPR requirements for SMEs so you should check whether any guidance has been or will be issued by your supervisory authority.

8. IS FILING OF DATA IN YOUR PC PROCESSING UNDER THE REGULATION?

Yes.

9. DOES THE GDPR APPLY ALSO TO AUTHORITIES?

Yes.

10. DO COMPANIES NEED TO STOP 'COLD CALLING' FROM LISTS THEY HAVE PREVIOUSLY OBTAINED? ARE THOSE LISTS A BREACH?

The processing of data for marketing purposes was subject to certain restrictions also under the previous legislation. Answering the question “are those lists a breach” could be misleading. The existence of lists is not a breach per se. The collection, use or transfer of such lists, however, might constitute a breach, depending on the specific circumstances.

11. DOES THE GDPR APPLY TO SHIPOWNERS THAT DON'T EMPLOY EU CREW?

This question presupposes that a ship owning business will only process crew's data, which in fact will never be the case. Article 3 par. 1 of GDPR provides that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This shall be the basic criterion for GDPR application in respect of any business.

12. HOW DO WE PROTECT MEDICAL DATA SENT TO AN EXTERNAL AGENT?

If the jurisdiction that the data is being transmitted to is not recognised by the Commission as having “adequacy” (acceptable safeguards for the protection of data) then transfers of data can be made where appropriate safeguards are provided by legally binding agreements / model contract clauses.

In essence, provisions should be written into the service agreement with the Agent detailing how the data must be protected, used and the conditions for erasure when no longer required for the purpose for which it was transmitted.

13. DO THE HANDLING/PROCESSING OF COMMERCIAL DATA (CIRCULARS OF CARGOES / VESSELS) FALL UNDER GDPR?

Not unless personal data is included in the commercial data.

14. DOES THE GDPR AFFECT THE DATA THAT A SHIP OF THE COMPANY USES AND SHARES?

Potentially yes. Application of the GDPR would depend on factors such as whether the data involved was personal data within the meaning of the GDPR, related to an EU citizen, and/or was processed by an organisation established in the EU.

15. WHAT PROVISIONS HAVE BEEN MADE FOR BANKRUPT COMPANIES HOLDING DATA?

It is expected that this would be governed by state-specific laws and would be the responsibility of the administrators or court appointed to deal with the bankruptcy. As such it will depend on the local jurisdiction.

16. WE ARE HEARING A LOT ABOUT INFORMATION/CYBER SECURITY AT THE MOMENT. HOW IS THIS DIFFERENT TO DATA PROTECTION AND HOW DO THESE THINGS FIT TOGETHER?

Having in place processes which comply with the GDPR is part of a robust information security framework, but information security also covers protection of other information and assets (for example financial or other commercial information) which may not necessarily be personal data but require protection nonetheless.

You should ensure GDPR-related procedures complement and fit into your information security framework appropriately and to minimise duplication of effort.

17. WOULD UBER BE IN BIGGER TROUBLE BEFORE OR AFTER GDPR?

57 million Uber users had their data breached including users in the EU. Uber attempted to hide this breach.

Under GDPR, Uber would be facing fines for any breaches of procedure that resulted in that loss and for failing to self-report with 72 hours of the controller becoming aware of the loss.

It is likely that any penalty would be greater for failing to self-report and given this was not a requirement under the Directive; it is likely their fine would be greater now under GDPR.

FAQS: GENERAL DATA PROTECTION REGULATION (GDPR)

JANUARY 2018

PENALTIES

18. WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Article 83 par. 4 of GDPR provides that the infringement of the provisions stipulated therein are subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Infringement of the provisions listed in the next paragraph (par. 5) of above article 83 of GDPR bring about double fines (i.e. 20,000,000 EUR or 4%). Article 84 of GDPR stipulates that Member States shall lay down the rules on other penalties applicable to infringements of GDPR in particular for infringements which are not subject to administrative fines pursuant to article 83.

19. WHAT HAPPENS IF THERE IS A GDPR BREACH BUT THE COMPANY IS UNAWARE AND DOES NOT REPORT? WOULD THEY STILL BE LIABLE TO A FINE EVEN IF THE CORRECT PROCEDURES ARE IN PLACE?

This depends on the circumstances of the breach and what processes you have in place within your organisation to prevent it occurring. An important element of these processes would be ensuring you have security measures in place to avoid breaches and are able to identify and respond to any breaches as soon as reasonably practicable.

If you were unaware of a breach for a period of time, you would need to investigate it and if appropriate report it as soon as you became aware of it.

When determining whether and to what extent you should be fined for a breach, regulators will consider matters such as how transparent you were in dealing with the breach, whether your processes are robust and appropriate, whether you should reasonably have become aware of the breach sooner, and whether your processes were operating properly.

20. COULD A MANAGEMENT COMPANY BE HELD LIABLE FOR MISHANDLING THE PEME DATA OF AN APPROVED P&I CLINIC?

Yes, potentially. This would depend on the circumstances.

21. CAN YOU APPEAL THE FINE IMPOSED BY THE DATA PROTECTION COMMISSIONER?

This would depend on the type of breach involved, the jurisdiction and the powers of the data protection commissioner within the jurisdiction.

CONSENT / LAWFUL USE

22. DO WE NOW NEED CONSENT FOR ALL HISTORICAL EMAIL LISTS?

See first the answer to question 23. Consent is only one of the grounds that allow you to lawfully hold and process personal data. If you can lawfully hold the information in an email list for other reasons, then consent will not be an issue.

The EU has yet to provide guidance on consent, this is due out shortly. The draft guidance which has gone out for consultation can be found here:

<https://www.ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>

The draft guidance notes state:

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But it's important to check your processes and records in detail to be sure existing consents meet the GDPR standard.

Recital 171 of the GDPR makes clear you can continue to rely on any existing consent that was given in line with the GDPR requirements, and there's no need to seek fresh consent.

However, you will need to be confident that your consent requests already met the GDPR standard and that consents

are properly documented. You will also need to put in place compliant mechanisms for individuals to withdraw their consent easily.

On the other hand, if existing DPA consents don't meet the GDPR's high standards or are poorly documented, you will need to seek fresh GDPR compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

23. IS CONSENT OF A DATA SUBJECT A PREREQUISITE ENABLING THE CONTROLLER TO PROCESS SUCH PERSONAL DATA? WHAT IS THE REMEDY IN THE CASE OF NON-CONSENT?

Lawful Reasons for Processing Data

Article 6 of the Regulation states processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

> Continued Overleaf

FAQS: GENERAL DATA PROTECTION REGULATION (GDPR)

JANUARY 2018

- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Analysis

If data processing falls under any one of heads (b), (c), (d) or (e) - then these will be "stand-alone" grounds and consent will not be needed.

Head (f) is more complex and this paper provides a useful analysis:

<https://www.theoriginaldatacompany.com/wp-content/uploads/gdpr-dpn-guidance.pdf>

Consent

Where consent is required, the request must be given in an intelligible and easily accessible form and must clearly state the purpose for processing the data, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Remedies

Pursuant to Article 79, where there are no lawful grounds for processing data, the data subject has the right to an effective

judicial remedy where he or she considers that his or her rights under GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with GDPR.

In addition, where there are no lawful grounds for processing the data, the data-subject has the right of erasure.

24. DO YOU REQUIRE EXPRESS CONSENT TO PROCESS PERSONAL DATA?

Not always. See the answer to Question 23.

Certain types of personal data will be required to enter into a contract of employment. In addition, financial regulations may mandate the holding of personal data. Express consent is only required if you cannot lawfully process data pursuant to the other five grounds in Article 6.

25. WILL THE GDPR APPLY TO DATA COLLECTED IN THE PAST? SAY A PRE-EMPLOYMENT MEDICAL RECORD OF 2011?

Yes.

26. DO OWNERS NEED TO REDRAFT ALL (CREW & EMPLOYEES ASHORE) OF THEIR EMPLOYMENT CONTRACTS (CLAUSES RE CONSENT, WITHDRAWAL ETC.)?

Owners should consider this; see response to question 23.

Owners will also need to ensure that individuals such as crew, employees and passengers are aware of which organisations Owners will be providing their personal data to (for example insurers and correspondents).

LIABILITIES

27. ARE GDPR FINES A P&I LIABILITY?

GDPR liabilities are not excluded from P&I cover, but the circumstances when a fine for breach of a GDPR breach might form the basis of a P&I claim are likely to be limited. Further, cover for such a fine would be discretionary and would require the Member to establish that the all reasonable steps to avoid the breach had been taken.

28. DOES CYBER INSURANCE COVER GDPR LIABILITIES?

This will depend upon the terms of the policy and you should consult your broker. At the present time, however, it appears that most cyber insurance policies would not cover fines for GDPR breaches.