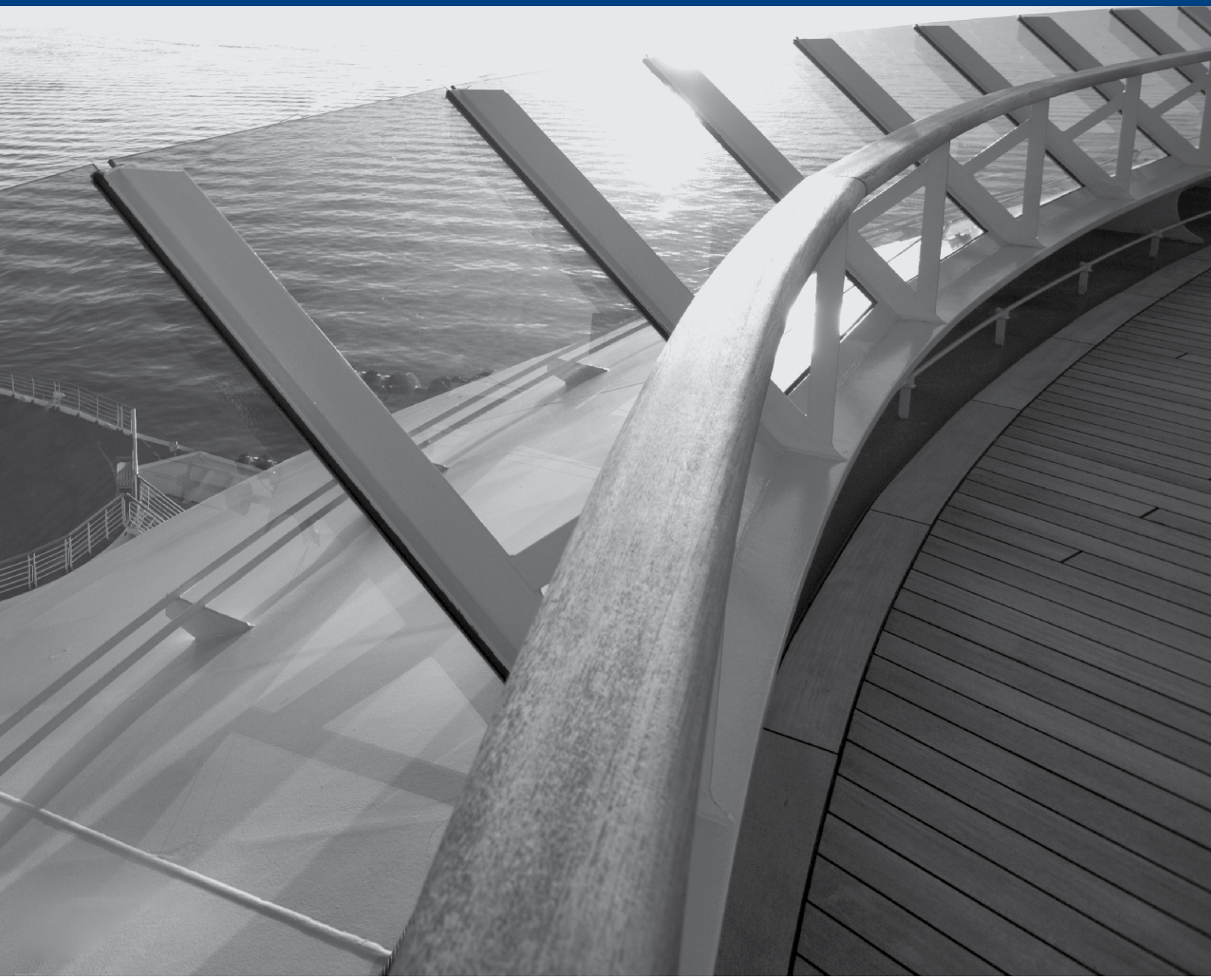


THE GDPR ICEBERG: DATA PROTECTION IN THE CRUISE INDUSTRY

The EU General Data Protection Regulation (GDPR), which overhauls a data protection regime dating from 1995, becomes effective across the European Economic Area (EEA), including in the UK, from 25 May 2018. It will apply to all businesses established in the EEA and a large number established outside of the EEA.

With large potential fines (the greater of up to 4% of global turnover or 20 million Euros), risk of claims from individuals and reputational damage, cruise lines, like all businesses, need to make the necessary changes to their systems and policies now in order to be prepared when the GDPR "goes live".

> “All EEA Member States (including the UK, regardless of Brexit) will have their own data protection laws to implement the terms of the GDPR and to set out their enforcement mechanisms.”

Cruise lines control a lot of personal data. They collect and store information about their passengers’ identities, preferences and health requirements. They hold information on their large workforces (whether employed or contracted). They have immigration law obligations in numerous jurisdictions. They conduct consumer-facing marketing campaigns. All of this information is likely to cross national borders and be exposed from time to time to physical and cyber security risk. The need to ensure data protection is already essential. Once the GDPR applies, and risk of large fines and reputational damage increases, a breach of the data protection rules could potentially sink the business (or at least cause it to take on water).

So what does the GDPR change and what stays the same?

The GDPR introduces a central theme of accountability which strengthens the existing rules, and the concept of “privacy by design”.

- It strengthens the existing rights of individuals and adds new rights.
- It introduces record keeping requirements and mandatory data breach reporting.
- It increases the information which must be notified to individuals and adds mandatory clauses to contracts between data controllers and data processors.

All of this means that, in practical terms, the obligations on data controllers will increase substantially. Businesses will require their counterparties to be compliant with the GDPR and data processors will also now have data protection obligations.

All EEA Member States (including the UK, regardless of Brexit) will have their own data protection laws to implement the terms of the GDPR and to set out their enforcement mechanisms. Germany, for example, approved a new Data Protection Act in May 2017 and the UK published on 14 September 2017 its draft of a new Data Protection Bill to implement the GDPR in the UK. Member States can tailor certain elements of the GDPR where this is permitted.

Application to international businesses

The GDPR will apply to organisations based outside of the EEA if certain conditions apply. The GDPR applies to a non EEA organisation if it has a presence in the EEA, or if it monitors the behaviour of individuals within the EEA (for example via cookies), or it offers services to individuals within the EEA. It also applies where EEA Member State law applies in accordance with international law, for example where a vessel is flagged with an EEA Member State registry. Particular factors to consider when determining whether the GDPR will apply are:

- Does your website refer to an EEA office?
- Do you have a registered establishment in the EEA?
- Is your website directed towards individuals based in the EEA, for example by giving an option to choose a “UK” or other member state setting, an EEA currency, or a particular EEA language?
- Is your business currently registered with an EEA data protection authority, such as the UK’s Information Commissioner’s Office (the ICO)?
- Do you use servers located in the EEA?
- Do you monitor the behaviour of any individuals within the EEA (irrespective of their nationality or habitual residence)? For example, if your website uses tracking cookies, then you are “monitoring individuals” for the purposes of the GDPR.
- Can your cruises be bought from within the EEA?
- Does the cruise depart from, visit or arrive in an EEA Member State?
- Are any of your vessels flagged within the EEA?

If the answer to any of these questions is yes, then it is likely that the GDPR applies to your business.

Eight key provisions of the GDPR which require action now

Having established that the GDPR will apply, consider the following eight provisions which require priority action. As a reminder, some key definitions are as follows: “data controllers” make decisions on how and why personal data is processed, whereas “data processors” only process data on the instructions of the data controller. “Processing” means essentially any action involving

personal data (including merely storing it). "Personal data" means any information relating to an identified or identifiable natural (living) person (data subject). Note that under the new definition of personal data, online identifiers such as cookies and IP addresses can make an individual "identifiable".

1. Grounds for processing – beware "consent"

As is currently the case, the processing of personal data is prohibited under the GDPR unless a data controller has one or more of the legal grounds set out in the legislation for processing the data. For standard personal data, the most useful of these grounds from a cruise line's point of view are:

- that the processing is necessary for the purposes of the "legitimate interests" of the data controller or a third party;
- that the 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;
- that the processing is necessary for compliance with a legal obligation; or
- that the individual has given his or her consent to the processing.

The grounds for processing sensitive personal data, such as health data, are more limited. With some exceptions, the individual's consent is necessary unless the individual's life is at risk (or other peoples' lives are at risk) and the individual is not able to give consent. Other grounds include processing which is necessary for reasons of substantial public interest on the basis of EU or Member State law, or processing which is necessary for the establishment, exercise or defence of legal claims, but these grounds can be difficult to rely on and must be carefully justified and documented. There are no applicable "legitimate interest"[1] or "necessary for the performance of a contract" grounds for sensitive personal data.

The GDPR tightens the "consent" ground for processing, which applies to both types of personal data but especially to sensitive personal data. The GDPR clarifies that, if relying on this ground, controllers must be able to demonstrate that an individual has consented to the processing of his or her data. Consent provisions cannot be buried in the middle of a long piece of text and must be a clear indication of the individual's wishes. In addition, the recitals to the GDPR clarify that consent must be able to be withdrawn at any time.

Action required

- If you currently rely on consent for processing any type of data (for example for direct marketing, special dietary or assistance requirements for passengers) you should check that all consents have been obtained and documented properly, or alternatively check whether there are other applicable grounds that you can rely on instead.
- Check that each individual on your marketing databases has either explicitly consented to receive electronic marketing, or, if they are existing customers, that they were given the opportunity to opt out from such marketing when their contact details were first collected, and that their wishes have been respected. Note that there will be specific provisions on electronic marketing in the forthcoming ePrivacy Regulation. As currently drafted, the proposed ePrivacy Regulation keeps the "soft opt in" currently available under the ePrivacy Directive for electronic marketing to natural persons. However, this is subject to change until the text is finalised.

2. Data audit and record keeping requirements

The GDPR will require data controllers (and processors) to keep records of the personal data they process. Once the Regulation becomes applicable there will be no phased implementation of the record keeping requirements. These records must be maintained, i.e. not just compiled but also updated. As a data controller, cruise lines' records must include, for example, the purposes of processing, the data subjects and categories of personal data involved, details of personal data transferred outside of the EEA, the envisaged time limits for deletion of different categories of data and a general description of the technical and organisational security measures it uses to keep personal data safe. These records must be available for inspection by a relevant EU data protection authority on request Where organisations have fewer than 250 employees the record-keeping requirements may not apply.

Action required

- Audit your personal data processing now. What personal data do you process? Why was it collected? Why and how are you using the data? Where is the data kept? Is there extensive personal data in archive? Do you still need all of it ? Do you use the data for the purpose it was collected or do you use it for new purposes?
- If personal data is out of date, update it. If personal data is no longer needed and you are not required by applicable law to keep it, delete it. This will minimise your risk and ensure that you are in compliance with the GDPR aim of personal data minimisation.

3. Fair processing notices

Data subjects must be kept informed about the processing of their personal data. The GDPR increases the amount of information which must be included in these notices. A key change is that, if the data controller is relying on its legitimate interests to process the personal data, the particular legitimate interests should be listed in the privacy notice.

1 There is a very limited *"legitimate interest"* ground for charities however.

Action required

- Add a privacy policy to your website, if you have not done so already, to make clear how you use data collected on your website, and also to make clear to passengers how their personal data will be used.
- Consider "just in time" notices (such as a box of text which appears when a mouse hovers over a particular box in a collection form) when collecting personal data such as email addresses to say how that information will be used.
- If you collect information on individuals from third parties then make sure that the individuals are aware that you are processing their data. Consider exploring contractual options to ensure that the individuals have been made aware that you will be processing the data, how and why, and how to contact you to enforce their rights.

4. Additional and strengthened rights for individuals

The GDPR strengthens and increases individuals' rights. Some examples are as follows:

- Subject access requests. The information which must be provided to an individual who makes a genuine subject access request has been increased (for example it must now include a notification of the right to lodge a complaint with the supervisory authority, and information about transfers of the data outside of the EEA). Organisations will have a shorter period of time to respond: the response must be "without delay" or at least within one month of receipt of the request (the current response period is 40 days).
- Right to request deletion. The controversial "right to be forgotten" has been strengthened, specifying the circumstances where the data controller must on request erase personal data without "undue delay" (for example where processing is based on the individual's consent but the individual has decided to withdraw that consent).
- Data portability. There is a new right to "data portability" for data which was provided directly by the individual, and where the processing is based on consent or on the carrying out of a contract. This applies only where the processing is carried out by automated means (for example, on computers). The data should be provided to the individual in a structured, commonly used and machine-readable format and the individual will have the right to transmit the data to another data controller.
- Right to object to processing. Individuals have a right under the GDPR to object to their data being processed where the processing is carried out using the legal grounds: (a) that the processing is necessary for the performance of a task carried out in the public interest; or (b) where the processing is necessary for the purposes of the legitimate interests of the controller or a third party. A data controller can continue to process the data if it can demonstrate *"compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject"* or if the processing is necessary for the establishment, exercise or defence of legal claims.
- Right to object to direct marketing. Individuals will have an absolute right to object to their personal data being processed (including storage) for direct marketing purposes. This is much stronger than the current right to object to receiving direct marketing materials, because it affects what data about individuals is stored, not just what can be done with it.
- Right to request restriction. Individuals will also have the right to request that their data be "restricted". This effectively means that a data controller will not be able to use the data in question until it has decided whether or not the individual's request is warranted or can be refused.

Action required

- Put processes in place to deal with requests from individuals seeking to enforce their rights within the shorter period permitted for response, including a designated team to deal with such requests. On receipt of a request from an individual, the quicker that you can make a decision the sooner you can resume business and minimise waste of company time and resources.

5. Contracts with processors

The GDPR requires that data controllers have contracts in place with their data processors, which must contain certain mandatory data protection clauses. Whilst the current law also requires data controllers to have contracts in place with data processors, all that is required at present is that processors act only on the instructions of controllers and that they have appropriate security measures in place to protect the data. Additional clauses required under the GDPR include, for example, an obligation on data processors to act only on the documented instructions of the data controller, to impose confidentiality obligations on the staff who will be processing the data and to delete or return all of the personal data at the end of the provision of services related to the processing.

Action required

- Consider which of your service providers and counterparties (such as tourist agencies, tour operators or cloud storage providers) are acting as data processors and which are acting as controllers or joint controllers; and
- Make sure that your contracts reflect the position and contain the necessary GDPR elements.

6. Reporting of personal data breaches

Notification of personal data breaches (e.g. cyber security breaches) to the relevant data protection authorities:

- Under the GDPR a data controller must notify a personal data breach to the relevant supervisory authority within 72 hours after becoming aware of a personal data security breach.
- The exception to this is where the personal data breach is *"unlikely to result in a risk to the rights and freedoms of natural persons"*.
- Where there is such a risk, a delay beyond 72 hours must be accompanied by reasons for the delay.

Notification to the individuals concerned:

- When the personal data breach is *"likely to result in a high risk to the rights and freedoms of natural persons"* the data controller must also notify the data subject *"without undue delay"*. This could be a smaller notification window than 72 hours.

This is a key change. The current EU Directive does not generally require data controllers to notify data protection authorities about security breaches (although telecommunications service providers are required to do so under the ePrivacy Directive and some Member State laws may require such notification). In the UK, the Information Commissioner's Office currently recommends that data controllers notify it if the breach poses a high risk to individuals but there is no legal requirement to do so (except for telecommunications service providers). Under the GDPR, notification is mandatory and as explained above the timelines are short for compliance.

In addition to the notification requirements, data controllers will need to keep a register of any personal data breaches, including details of what happened and what was done to resolve the issue. This will be subject to inspection by the relevant supervisory authority, for example the UK's Information Commissioner's Office.

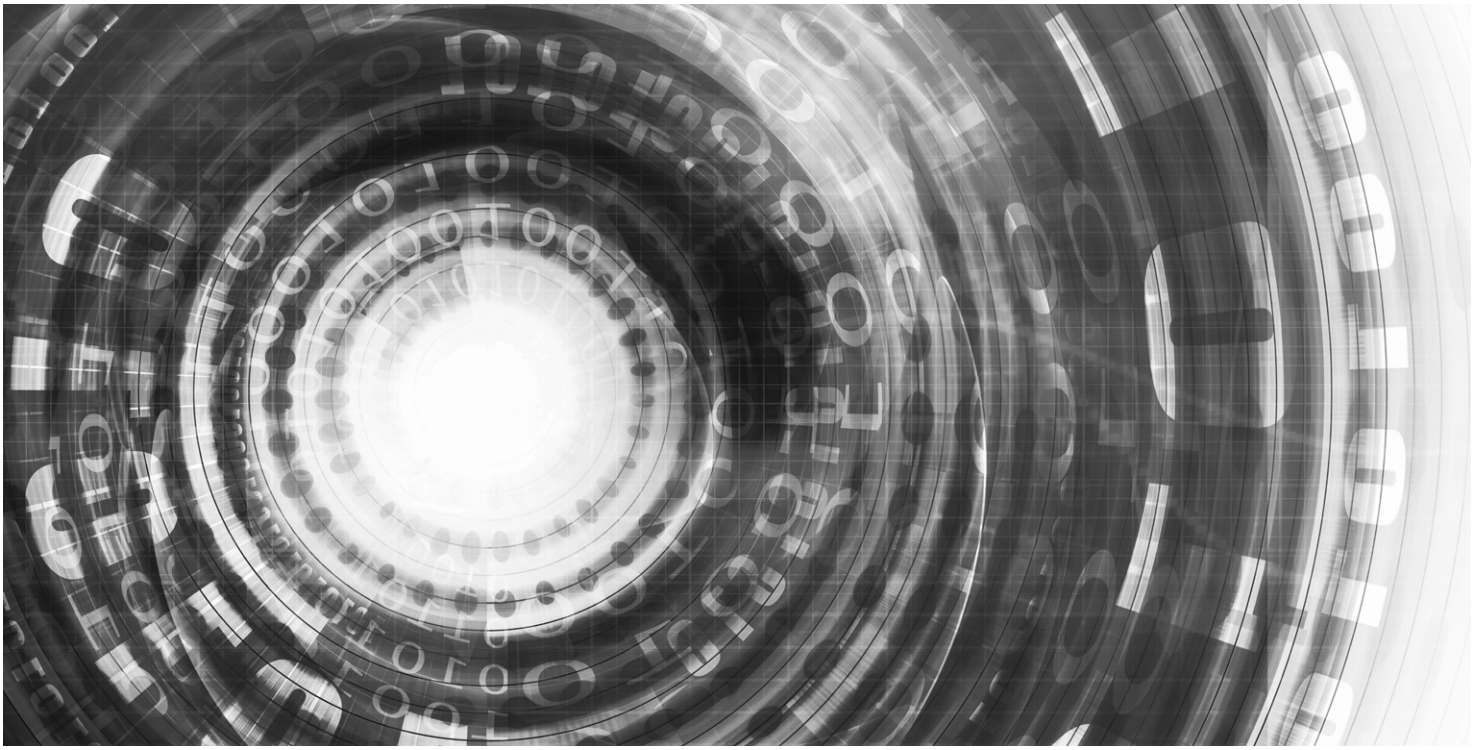
Action required?

- Create and maintain a register of data breaches.
- Update your cyber security breach procedure to take into account the short timelines for notification under the GDPR.
- If you do not already have such a procedure in place, consider creating one. In the event of a security breach there will be very little time in which to determine the extent of the damage, the individuals affected, the security arrangements which will need to be either changed or strengthened, and whether or not the breach requires notification to the national data protection authority and/or individuals concerned. It would be prudent to establish parameters for making such decisions, and people who will be responsible for making them.
- Consider taking out a cyber insurance policy and lining up public relations advisors who can help you to reduce the damage to your reputation in the event of a personal data breach.

7. "Privacy by design" and Data Privacy Impact Assessments

An important new concept is that of "privacy by design" and by default. When introducing new products, services, or processes, data controllers will need to show that the impact of such products, services or processes has been considered, and that steps have been taken to minimise any negative impact on individuals' rights and freedoms. Data should be "pseudonymised" where possible (and where anonymisation is not possible), for example replacing a passenger's name with "passenger 1234". Data should also not be collected unless really needed.

"Consider taking out a cyber insurance policy and lining up public relations advisors who can help you to reduce the damage to your reputation in the event of a personal data breach."



Action required?

- Do not collect personal data unless you can justify your purposes for doing so and you have conducted and documented privacy impact assessments. These should, amongst other things, determine how you will keep personal data safe and how high risk the proposed project is to individuals' privacy.
- Make sure that your data protection policies are up to date and that your data processing is transparent.

8. Appointment of Data Protection Officers

Although there will no longer be a need to register as a data controller in an EU Member State, data controllers and processors must designate a "data protection officer" in certain circumstances, including where:

- "*The core activities*" of the controller or the processor consist of *"processing operations which… require regular and systematic monitoring of data subjects on a large scale"*; or
- The "core activities" of the controller or the processor consist of *"processing on a large scale"* of *"special categories of data"* (i.e. "sensitive personal data") and "personal data relating to criminal convictions and offences".

The GDPR does not define what "large scale" means and it is not clear from the current guidelines when the obligation arises. However, bearing in mind that *"regular and systematic monitoring"* will include CCTV monitoring of public areas on board cruise ships, we recommend that even smaller cruise lines consider carefully whether their processing of personal data (including sensitive personal data) will give rise to a requirement for designation of a data protection officer.

A controller or processor can also choose to appoint a data protection officer voluntarily. Or a Member State can require it under local law. Given the increasing importance of data protection and the high profile of the cruise industry, it may well be a prudent investment to dedicate appropriate resources for timely compliance with applicable data protection laws. It may be sensible for a cruise line to appoint a data protection officer even where it is not yet clear that this is strictly required by the GDPR (or by implementing legislation of EU Member States).

However, if a cruise line does decide to appoint a data protection officer it should be mindful that the data protection officer should have expertise on both local (i.e. relevant EU Member State) data protection law and on the GDPR.

Action required

- Assess whether you should appoint a data protection officer, and make arrangements accordingly. Note that the data protection officer should have expertise on both local data protection law and on the GDPR.

Position of travel agents

Travel agents are likely to be considered "data controllers" in their own right where they make decisions themselves about how and why to process personal data of passengers or prospective passengers. Where travel agents are data controllers they have the same obligations under the GDPR that the cruise lines will have (subject to variations in applicable Member State law, depending on the location of the travel agent).

Conversely, where travel agents process certain personal data only on behalf of cruise lines, for that

"The penalties for getting this wrong are potentially very high. EEA supervisory authorities will have the power to impose fines of up to 20 million Euros, or 4% of the total worldwide turnover of a business in the preceding financial year, whichever is higher."

particular processing the travel agents may be data processors. Data processors have some obligations under the GDPR but do not have all of the obligations that data controllers have. If a data processor processes personal data in a way which causes a cruise line to breach its obligations under the GDPR then the cruise line may be held liable for that breach unless it can show that it is not responsible in any way.

Whether a travel agent is a controller or a processor will depend on the circumstances and should be carefully considered.

Action required

- Develop policies to ensure that the position is clear at the outset of any commercial relationship with a travel agent, and that the cruise line is adequately protected.

Why should international cruise lines comply with the GDPR?

Privacy rules around the world are tightening. The GDPR is just one example of a regime change which aims to put individuals' privacy rights first. Many of the principles are similar in laws around the world, but the GDPR is often stricter. Although compliance with the GDPR will not guarantee compliance with all privacy regimes across the globe, it will help to reduce global risk.

A cruise line which safeguards its passengers' (and employees') privacy rights will also be more likely to attract and retain its customers. Marketing will be more effective when it does not target individuals who do not want to be contacted. Campaigns will be better equipped to gain and maintain the trust of customers and employees alike.

Note that the GDPR will also apply to a number of airlines. Please see HFW's separate bulletin for airline clients which will be published soon and will be available from hfw.com.

As discussed above, the penalties for getting this wrong are potentially very high. EEA supervisory authorities will have the power to impose fines of up to 20 million Euros, or 4% of the total worldwide turnover of a business in the preceding financial year, whichever is higher. Add to the risk of fines the risk of complaints and even claims from unhappy customers and the reputational damage involved in breaching data protection law.

EEA Member States must also lay down rules on other penalties applicable to infringements of the Regulation, and must take *"all measures necessary to ensure that they are implemented… such penalties shall be effective, proportionate and dissuasive"*. Under the UK's draft Data Protection Bill, which will implement the GDPR in the UK, Directors will have personal liability for some criminal offences.

There is still time to prepare for the GDPR before it becomes applicable on 25 May 2018 but the clock is ticking.

For further information please contact:

ELINOR DAUTLICH
Partner, London
T +44 (0)20 7264 8493
E elinor.dautlich@hfw.com

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

WILLIAM MACLACHLAN
Senior Associate, London
T +44 (0)20 7264 8007
E william.maclachlan@hfw.com

FELICITY BURLING
Associate, London
T +44 (0)20 7264 8057
E felicity.burling@hfw.com

HFW has over 500 lawyers working in offices across Australia, Asia, the Middle East, Europe and the Americas. For further information about our EU, competition and trade regulatory capabilities, please visit hfw.com/EU-Competition-and-Regulatory

hfw.com

Beirut Brussels Dubai Geneva Hong Kong Houston Kuwait London Melbourne Paris Perth Piraeus Riyadh São Paulo Shanghai Singapore Sydney