AVOIDING THE GDPR ICEBERG – DATA PROTECTION IN THE SHIPPING INDUSTRY

Businesses now have less than nine months to prepare for the EU General Data Protection Regulation (GDPR), which overhauls a data protection regime dating from 1995. The GDPR becomes effective across the European Economic Area (EEA), including in the UK, from 25 May 2018. It will also apply to a large number of businesses 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, businesses need to make the necessary changes to their systems and policies now in order to be prepared when the GDPR "goes live" on 25 May 2018.

"Immigration law obligations in numerous jurisdictions require certain personal information to be shared. Every business transaction involves interaction with individuals working for corporate counterparties. Much of this information is likely to cross national borders and be exposed from time to time to physical and cyber security risk."

Organisations in the shipping industry may collect a lot of personal data, from email addresses of business contacts and counterparties to vessel crew and passenger information, as well as information about their own employees. Crew and contractors are vetted and managed. Immigration law obligations in numerous jurisdictions require certain personal information to be shared. Every business transaction involves interaction with individuals working for corporate counterparties. Much of this information is likely to cross national borders and be exposed from time to time to physical and cyber security risk. Once the GDPR applies, and the risk of large fines and reputational damage increases, breach of the data protection rules could potentially sink the business (or at least cause it to take on water).

Does the GDPR apply to my business if it is not based in the EEA?

The GDPR applies to all organisations "established" within the EEA, i.e. any organisation which has a "real and effective activity, even a minimal one, exercised through stable arrangements". If you have an office or regular operations in the EEA, and process personal data in the context of that office or those operations, then the GDPR is likely to apply to your business. The fact that the processing itself actually takes place outside of the EEA would not be material.

The GDPR will also apply to organisations established outside of the EEA if certain conditions apply, including where they monitor the behaviour of individuals within the EEA (for example, via cookies), offer goods or services to individuals within the EEA (note that if you offer goods or services to a business that business has individuals within it) or where EEA Member State law applies in accordance with international law, e.g. where a vessel is flagged with an EEA Member State registry.

Particular factors to consider when determining whether the GDPR will apply are:

- Are any of your vessels flagged within the EEA?
- Is your website directed towards customers based in the EEA, for example by giving an option to choose a "UK" setting, an EEA currency, or a particular language?
- Can your services be bought from within the EEA?
- Do you have a registered establishment or an office in the EEA?
- 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.

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

So the GDPR applies to my business – what next?

The GDPR introduces a host of new obligations and requirements with which businesses must comply.

First, some essential terminology: "data controllers" make the decisions on how and why personal data are processed. "Data processors" only process data on the instructions of the data controller. "Processing" means any action involving personal data, including merely storing it. "Personal data" means any information relating to an identified or identifiable natural (living) person (a "data subject"). Under the new definition of personal data, online "identifiers" such as cookies and IP addresses can make an individual "identifiable". "Sensitive" or "special category" reveal information such as an individual's health, race or ethnicity, religious beliefs, ethnicity or sexual orientation.

A full list on how to comply with the GDPR requires more space than is available here, but five key action points are as follows:

1 Conduct a data audit. Data controllers and processors alike are required to keep records of their personal data processing. Analyse your systems and practices to check what personal data you process, why, how you use them, where they are stored and whether you still need them. Check whether you process them in accordance with one of the permitted legal grounds (e.g. has the individual given their consent, or is the processing necessary for the performance of a contract with the individual, or necessary for a legitimate business interest). "Sensitive" personal data are subject to stricter rules and processing usually requires the individual's consent. Note that "consent" is more difficult to obtain under the GDPR regime than under the UK Data Protection Act 1998 which implements the current EU data protection regime. Criminal records of employees or service providers can only be processed in accordance with specific EEA Member State laws. Document your findings and decisions.

2 Draft or amend policies and procedures. The GDPR strengthens and adds to individuals' rights, for example it strengthens the rights to have personal data deleted or frozen, adds a new right of "data portability" where an individual can request that personal data stored electronically be transferred to a different data controller, and shortens timelines for compliance with individuals' requests. It also imposes new obligations on all data controllers to report personal data breaches to relevant data protection authorities within 72 hours, and to report breaches to individuals concerned (if the breach is high risk) "without undue delay". It introduces a new concept of "privacy by design", which requires businesses to think about protecting individuals' privacy at the very beginning of any new project and to conduct "privacy impact assessments" calculating the potential risks to individuals' privacy rights. Businesses will need to update (or draft) policies and procedures to ensure compliance with these obligations.

3 Inform individuals about your processing through fair processing notices. Individuals 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. Privacy policies will need to be updated and businesses will need to amend (or draft) notification forms.

4 Amend or put contracts in place with data processors. The GDPR requires data controllers to have contracts in place with all of their data processors, containing certain elements specified in the GDPR.

5 Appoint a data protection officer. Many businesses will be required to appoint data protection officers, or may choose to do so voluntarily, given the increased risks associated with data protection.

These are just some of the actions that organisations need to take now. For more information on how you can prepare, and what systems you must have in place, see our special GDPR update at https://goo.gl/jNjMym or contact either:

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

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

The GDPR becomes applicable from 25 May 2018. There is still time to prepare but the clock is ticking: don't wait to start your GDPR project.

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 regulation 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