LOSS PREVENTION Briefing

NORTH SERVICE, STRENGTH, QUALITY

LOSS PREVENTION BRIEFING FOR NORTH MEMBERS LEGAL / AUGUST 2017

General Data Protection Regulation Explained

Contents

Introduction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. Any organisation which provides services or handles data relating to EU citizens, including employees, is required to comply with the GDPR. Some of the changes made by the GDPR are significant and penalties can be very severe. Having in place an appropriate data protection framework is also important in light of the increasing threats posed by cyberattacks. This briefing provides a short overview of the GDPR together with some practical compliance measures to consider.

What is the GDPR?

It is a new piece of EU legislation introduced to protect personal data about individuals. It will introduce a data protection framework which will apply across all EU member states. Organisations which the GDPR applies to will be subject to the oversight of the data protection authority situated in the EU member state where the majority of their operations are situated or take place (**relevant data protection authority**).

What is Personal Data?

Personal data is any information relating to a person who can be identified by an identifier such as a name, identification number, location data, online identifier or through specific factors relating to their biological or social identity. **Special category** personal data is data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, genetic, medical or orientation. There are additional restrictions when processing these types of data.

General Data Protection Regulation

What Does 'Processing' Personal Data Mean?

Processing is performing any operation on one or more item of personal data. Examples are automated activities (such as generating a mailing list from a database) as well as amending, searching for, using, disclosing, erasing or deleting personal data.

What are Data Controllers and Data Processors?

A **data controller** is the organisation which, either alone or jointly with others, determines the purposes and means of the processing of personal data. If your organisation uses any personal data for any commercial purpose, it is likely that you are the controller of some or all of that information.

A **data processor** undertakes **processing** of personal data on behalf of a **controller.** Note that GDPR obligations apply to processors as well as controllers.

When Does the GDPR Come Into Force?

It comes into force on 25 May 2018.

Who Does it Apply to?

It applies to any organisation that provides services to, or handles data about, EU citizens. This is the case even if a company is not physically located or incorporated in an EU member state.

Why Has the GDPR Been Introduced?

It updates and enhances current legislation in recognition of the increase in globalisation, technological developments, digitalisation and e-commerce which have occurred in recent years and continue to occur. It is also intended to protect individuals from unauthorised use and potential exploitation of their personal information by companies.

It increases harmonisation in standards between EU member states and, due to the fact that it applies to organisations located outside of the EU if they are handling personal data about EU citizens, expands the territorial reach of the legislation to increase the protection it provides to EU citizens.

What are the Consequences of not Complying with the GDPR?

Organisations can be fined up to the greater of 2% of annual worldwide turnover or €10million, or the greater of 4% of annual worldwide turnover or €20million for more serious breaches. Demonstrating GDPR compliance, or declaring non-compliance, may form part of the application process for EU public contract tenders or may be a requirement when contracting with companies situated in the EU. There are also the obvious reputational consequences of a data breach.

Key Requirements

Processing personal data must be lawful, fair and transparent.

Processing personal data is only permitted if:-

- Consent has been obtained; or
- The processing is **necessary** and an appropriate privacy notice has been provided.

Processing is **necessary** if it is undertaken to meet at least one of the following criteria:-

- **Perform a contract** with the individual;
- **Comply** with a legal obligation;
- **Protect** the vital interests of the individual or another person;
- **Perform a task in the public interest**;
- Allow your organisation to pursue its **legitimate interests**, provided these are not overridden by fundamental rights of the individual such as the right to privacy.

The requirements are more onerous where special category data is involved, and normally the individual's explicit consent will be needed.

General Data Protection Regulation

Privacy Notices

Where your organisation is the **controller** and has obtained personal data either directly from the relevant individual or from a third party, you must provide the individual with a privacy notice.

If you obtain the information directly from the individual, this must be done at the time of obtaining the personal data.

If you obtain the information from a third party, such as an agent or a contractor, you must provide the privacy notice as soon as reasonably practicable after receiving the information, at the time of first communication with the individual or disclosure to a third party as applicable, but within one month of receipt at the latest. This requirement has relatively significant implications for organisations as there may be situations where in practice it is difficult or impossible to issue the privacy notice to individuals if your organisation does not have contact details for them. In such situations it may be necessary to provide the third party with a copy of the relevant privacy notice and include wording in your contract with them to require them to issue the privacy notice on behalf of your organisation. However, be aware that if you take this approach your organisation will still be accountable for this requirement under the GDPR.

The privacy notice provided must contain:-

- The identity and contact details of your organisation;
- The contact details of your data protection officer, if you have one;
- The purposes of processing the data;
- The **legal basis** for the processing (consent or necessity as set out above). Note that if you rely on the legitimate interests legal basis, you must describe what the legitimate interests are;
- An explanation of who will receive the personal data, including any third parties; and
- Where applicable, reference to the fact that your organisation plans to transfer the data to a country or organisation outside of the EU and a description of how the data will be appropriately safeguarded;
- Details of how long the data will be stored for or if this is not known a description of how your organisation determines how long data is stored for;
- Details of the individual's right to request access to and rectification of their data, or to request restriction of processing of their data;
- Explanation of the individual's right to lodge a complaint with an EU data protection authority;
- Whether providing the data is a legal requirement or necessary to perform or enter into a contract, as well as whether providing the data is optional and any consequences of failure to provide it; and
- Details of any automated or profiling processes applied to the personal data.

Individual Rights

Individuals have an express right to:-

- request details of data about them held and processed by your organisation, as well as information about who this has been disclosed to or where the data was received from. You are required to provide a copy of this data; and

- object to processing of their personal information. This specifically includes direct marketing.

Data Portability

Individuals have the right to request a copy of personal data held by an organisation which relates to them, or to request the organisation to transfer the information to another organisation. The information held about them must be provided in a structured, commonly used format which can be used by IT applications. This is designed to promote competition between goods and service providers by making it simple to switch between providers.

Where a request is made for data to be transferred to a third party, it is important to verify the identity of the individual making the request and confirm it is genuine.

Right to be Forgotten

Individuals now have the right to request their data to be rectified or erased without undue delay, or restrict the processing of it, where:-

- the information is no longer necessary;
- the data has been unlawfully processed; or
- consent to the processing has been withdrawn.

This is known as the 'right to be forgotten'. Requests of this nature must be complied with unless and to the extent that there is a specific legal or public interest reason why this is not possible, or where the information is required for the establishment, exercise or defence of legal claims.

If the individual is not happy about any of these matters, they are able to complain to a data protection authority.

Data Protection Officer

Organisations will be required to appoint a data protection officer if the organisation undertakes large scale monitoring of individuals or large scale processing of **special category data**, including data about criminal convictions and offences. The data protection officer must have expert knowledge of data protection law and practice. The role must be independent from operations to enable them to provide appropriate oversight. The data protection officer's contact details must be published. The GDPR contains prescribed obligations which the data protection officer must undertake.

Accountability and Appropriate Organisational Measures

It is a specific requirement to implement appropriate technical and organisational measures to protect personal data and to ensure that only necessary processing takes place. This includes:-

- Ensuring that the amount and extent of processing of data collected is not excessive;
- Data is not retained for longer than is necessary;
- Data is not more accessible than is reasonably required.

Transferring data to a country outside the EU (a third country)

Organisations subject to the GDPR are only permitted to transfer data to a third country in the following circumstances:-

- The third country (or a specified sector or territory within that country which you would be transferring the data to) has been designated by the European Commission as having an adequate level of personal data protection;
- Appropriate data safeguards are in place, which are legally binding and enforceable. For intra-group overseas transfers these should be set out in binding corporate rules, which will document the group structure, what data is transferred, roles and responsibilities, the legal basis for the processing and what measures are in place to protect the data and ensure individuals can enforce their rights in respect of the data;
- The individual has explicitly consented to the third country transfer, having been informed of the possible privacy risks arising out of there being no adequacy or appropriate safeguards in place;
- The transfer is necessary for the performance or entry into a contract, public interest purposes, legal claims process, to protect the vital interests of the individual or other people; or
- If none of the options above is available, the transfer may be permitted if only a small number of individuals are affected provided the relevant data protection authority has been informed.

What to do In the Event of a Data Breach

A personal data breach is wider than simply losing personal data. It means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Unless the breach is minor and would not threaten the privacy of any individual (for example if the information was in an encrypted form which would not be intelligible to a person not authorised to view it), the GDPR requires organisations to notify the relevant data protection authority within 72 hours of becoming aware of the breach. If there is a delay in notification, the reasons for this must be explained.

It is important to have in place a data breach response procedure which sets out measures taken to address the breach and/or to mitigate potential adverse effects of it. The procedure should also set out when notification to data protection authorities is required and what information should be included in the notices. Other necessary steps should also be detailed in this procedure, such as agreeing a public relations strategy, initiating an investigation to identify the cause of the breach and to recommend remedial action to prevent future breaches, notifying your board and, if appropriate, other stakeholders, and notifying your corporate insurers.

General Data Protection Regulation

Practical steps towards GDPR compliance

- Set up a working group to review the GDPR and consider the implications. Ensure you also review any state-level legislation or guidance supplemental to the GDPR which is applicable to you. Generally this will be headed by your legal, compliance or HR team but all operational areas, including marketing and communications, should be represented. Your IT function will also need to be involved.

- Clarify who your **relevant data protection authority** will be.

- Undertake a data protection audit: assess what personal data each department or business area within your organisation holds, what this is used for and how it is stored/destroyed. This can be overseen/conducted by your working group or alternatively you could consider instructing a legal or professional firm.

- Using the results of your data protection audit, produce a matrix of all personal data your organisation processes, who/where you receive it from and who you share it with. This should provide a starting point for producing your privacy notice(s).

- Draft privacy notice(s). You may need more than one privacy notice, for example one which contains consent wording where special category data is collected, one for commercial use and one for human resources and recruitment matters. Where you are relying on the individual's consent, make sure that the consent received is recorded.

- Update group policies and procedures to comply with the GDPR.

- Have in place document retention policies which require archiving and destruction of information once the relevant legal limitation period has expired.

- Consider the impact of the right for individuals to request access to data held about them in the context of customer information systems and records; staff should be provided with guidance to ensure that they are aware that personal or subjective views recorded about individuals may need to be shared with those individuals on request.

- Review key contracts to assess whether they contain appropriate data protection obligations.

- Assess whether your organisation's information security framework is robust enough to reduce the risk of unauthorised disclosure of personal information. Ensure you consider cyber attack exposures as part of this process, and assess whether your cyber insurance and business interruption insurance policies provide sufficient protection.

- Establish a data breach procedure which sets out steps to take in the event of a data breach.

- Ensure all staff are trained about the GDPR requirements and any updated documents and procedures before the GDPR comes into force.

- Direct marketing: ensure records are kept where direct marketing is objected to so that the information is no longer processed for this purpose in accordance with the individual's wishes. Records must also be kept of instances where consent to processing of personal data has been withdrawn, and there should be a process for notifying relevant departments within the organisation when this occurs.

- Be aware of the consent requirements: ensure a written consent declaration is obtained, which must be freely given, easily accessible and in clear and plain language. Retain a copy of the consent; if consent is withdrawn ensure that records are updated immediately so that no further processing of the data takes place.

- Undertake a privacy impact assessment if you intend to undertake new processing activities, or to use new or different technology to undertake the processing you currently do. Note that where the proposed processing would pose a high risk to individuals' privacy, prior consultation with the **relevant data protection authority** is required.

Finally: keep in mind the principles of the GDPR. Organisations should collect and handle personal data only when they need to and ensure this is done lawfully, fairly and transparently. A benchmark to apply is whether you would be happy if someone else collected or used personal data about you in the same way as you propose to.

Disclaimer

The purpose of this publication is to provide a source of information which is additional to that available to the maritime industry from regulatory, advisory, and consultative organisations. Whilst care is taken to ensure the accuracy of any information made available no warranty of accuracy is given and users of that information are to be responsible for satisfying themselves that the information is relevant and suitable for the purposes to which it is applied. In no circumstances whatsoever shall North be liable to any person whatsoever for any loss or damage whensoever or howsoever arising out of or in connection with the supply (including negligent supply) or use of information.

Unless the contrary is indicated, all articles are written with reference to English Law. However it should be noted that the content of this publication does not constitute legal advice and should not be construed as such. Members should contact North for specific advice on particular matters.

The North of England P&I Association The Quayside, Newcastle upon Tyne, NE1 3DU, UK

Telephone: +44 191 2325221 Facsimile: +44 191 261 0540 Email: loss.prevention@nepia.com www.nepia.com