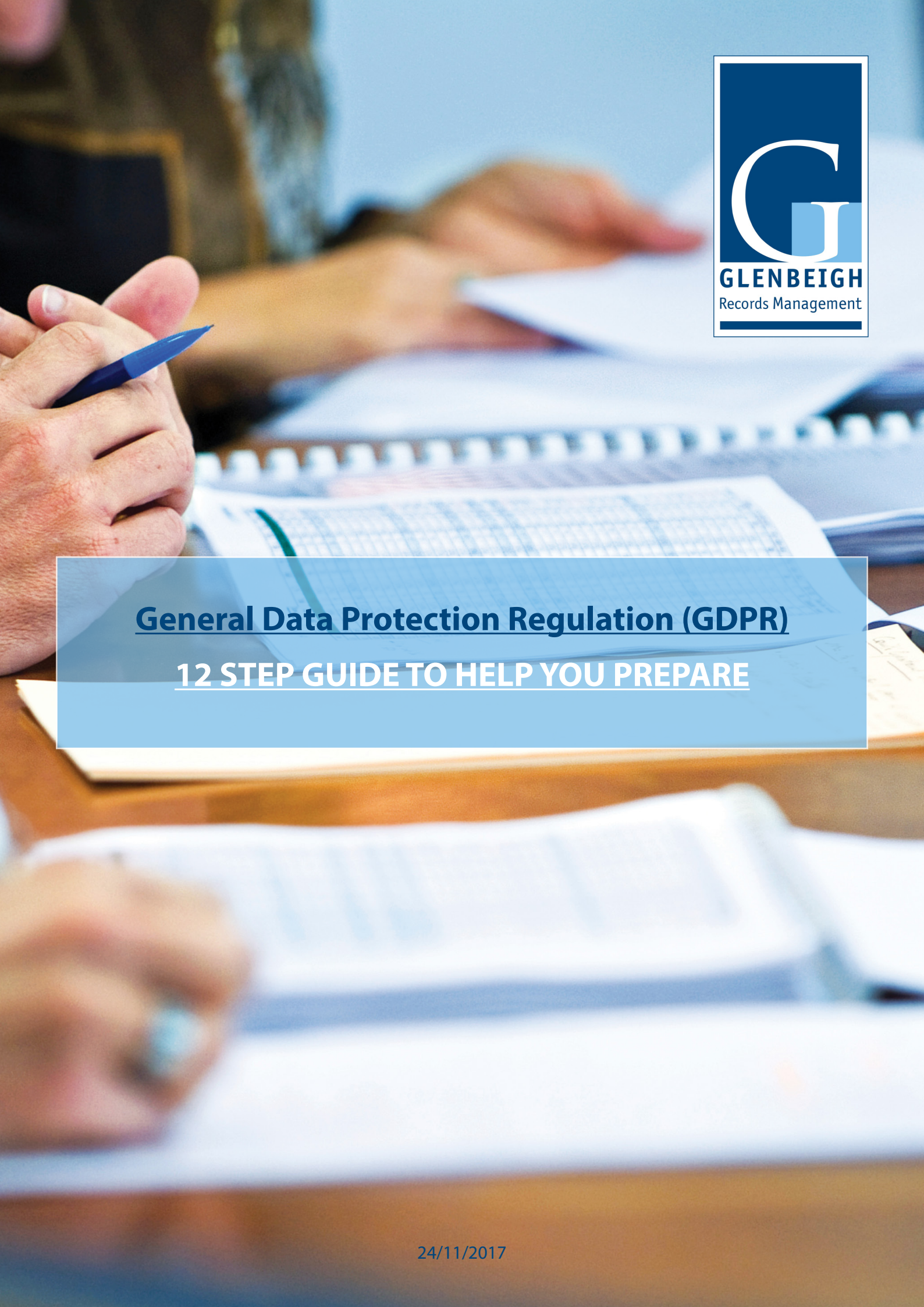

GLENBEIGH
Records Management

General Data Protection Regulation (GDPR)

12 STEP GUIDE TO HELP YOU PREPARE

24/11/2017

WHAT YOU NEED TO KNOW

GDPR builds on the main concepts and principles in the EU Data Protection Directive 95/46/EC. It contains however significant enhancements and new elements, therefore organisations will have to do some things differently or implement new processes for the first time.

Depending on your type of organisation GPDR compliance may have budgetary, personnel, IT, governance and communications implications. Therefore, it is imperative that you plan your approach as soon as possible. A good starting point would be map out which parts of GDPR will have the greatest impact on your business and give those areas due prominence in your planning process.

Outlined below are twelve steps that will help you prepare for compliance. Please note that this guide is for informational purposes only and should not be relied upon as legal advice. We encourage you to work with legal professionals to determine precisely how the GDPR might apply to your organisation.

1). AWARENESS

Key management personnel should be made aware that GDPR comes into force on 25 May 2018. They need to be aware of the impact this is likely to have and identify areas that could cause compliance issues.

It would be useful to start looking at your organisation's risk management processes, as implementing GDPR could have significant resources issues. Achieving compliance ahead of the enforcement date may become difficult if you leave your preparations until the last minute.

2). BECOMING ACCOUNTABLE FOR THE INFORMATION YOU HOLD

You should examine the personal data you hold and document the following:

- Why was it originally gathered?
- Where it came from?
- Why are you holding it?
- How long will you retain it for?
- It is shared with third parties and on what basis?
- What security is in place to protect this personal data, both in terms of encryption and accessibility?

Conducting this review will help you comply with GDPR's accountability principle, which requires organisations to demonstrate the ways in which they comply with the data protection principles.

GDPR requires organisations to maintain records of their processing* activities. It updates rights for a networked world therefore if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records.

3). COMMUNICATING PRIVACY INFORMATION

At present, if you collect personal data you have to provide individuals with certain information, such as your identity, why you are gathering the data, how you intent to use it, who it will be disclosed to, and if it's going to be transferred outside the EU. This is usually done through a privacy notice. GDPR will require organisations to communicate additional information to individuals prior to processing their personal data, this includes:

- The legal basis for processing the data
- The data retention periods
- The right to complain to the Data Protection Authority if they think there is a problem with the way you are handling their data
- Whether the data will be subject to automated decision making
- The rights individuals have under GDPR

You should therefore review your privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. All information communicated must be provided in clear language that is concise and easy to understand.

4). INDIVIDUALS' RIGHTS

GDPR includes the following rights for individuals:

- The right to be informed
- The right to access
- The right to rectification
- The right to have information erased
- The right to restrict processing
- The right to object to direct marketing
- The right not to be subject to automate decision-making including profiling

You should therefore review your procedures to ensure they comply with all the rights individuals have. This review should also consider the following:

- How long does it take to locate (and correct or delete) the data from all locations where it is stored?
- Who will make the decisions about deletion?

The right to data portability is new and only applies:

- to personal data an individual has provided to a controller**;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

It will require organisations to provide data electronically and in a commonly used format free of charge.

Individuals may exercise their rights at any time so it is essential that organisations are prepared.

5). SUBJECT ACCESS REQUESTS

Organisations will need to plan how they handle requests under the new rules and put in place procedures. Access requests must be concluded within one month therefore there should be no undue delay in processing. Charges cannot be applied for processing an access request, unless you can demonstrate that the cost will be excessive. Only if an access request is deemed to be manifestly unfounded or excessive it can be refused. A refusal policy must be in place and the organisation will have to demonstrate that the access request meets the refusal policy criteria.

You will also need to provide some additional information to people making requests, such as your data retention periods and the right to have inaccurate data corrected. If your organisation handles a large number of access requests, the impact of the changes could be considerable. The logistical implications of having to deal with requests in a shorter timeframe and provide additional information will need to be factored into future planning for organisations. It could ultimately save your organisation a great deal of administrative cost if you can develop systems that allow people to access their information easily online.

6). 'LEGAL BASIS' FOR PROCESSING PERSONAL DATA

Organisations should identify their legal basis for processing data and document it. This will help them comply with GDPR's 'accountability' requirements, it will assist them in preparing their privacy notice, and it will help them answer subject access requests as the legal basis for processing personal data needs to be outlined in the response. If consent is relied upon as the sole legal basis for processing data then organisations should be prepared for individuals requesting that their personal data be deleted.

GDPR reduces the number of legal bases government departments and agencies may rely on when processing data. Instead, they will have to have specific legislative provisions underpinning one or more of the methods used to process data.

All organisations need to carefully consider how much personal data they gather. If any categories can be discontinued they should be. Then they should consider whether the remaining data needs to be kept in its raw format or how quickly can they begin the process of anonymization and pseudonymisation.

7). CUSTOMER CONSENT

Consent must be freely given, specific, informed and unambiguous. It cannot be inferred from silence, pre-ticked boxes or inactivity – there must be a positive indication of agreement. You should therefore review how you seek, obtain and record consent, and determine if you need to make any changes.

If consent is the legal basis relied upon to process personal data, you must make sure it will meet the standards required by GDPR. If it does not, then you should amend your consent mechanisms or find an alternative legal basis. Consent needs to be verifiable and individuals must be informed in advance of their right to withdraw consent at any time.

8). PROCESSING CHILDRENS' DATA

If your organisation processes data from underage subjects you must ensure that you have adequate systems in place to verify individual ages and gather consent from guardians.

GDPR introduces special protections for children's data, particularly in the context of social media and commercial internet services. Each EU state will define the age up to which an organisation must obtain consent from a guardian before processing a child's data. If a child is younger then you will need to get consent from a person holding 'parental responsibility'. This will have significant implications on organisations that offer online services to children and collects their personal data. It should be noted that consent needs to be verifiable, and therefore communicated to underage customers in language they can understand.

9). REPORTING DATA BREACHES

GDPR introduces a duty on all organisations to report all data breaches to the Data Protection Authority within 72 hours of a breach

occurring. Breaches that are likely to bring harm to an individual must also be reported to the individuals concerned, for example, identity theft or a breach of confidentiality.
You should therefore put procedures in place to detect, report and investigate a personal data breach. It is worth noting that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10). DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. This means that service settings must be automatically privacy friendly, and requires that the development of services and products takes account of privacy considerations from the outset.

The regulation introduces mandatory Data Protection Impact Assessments (DPIA) for organisations where privacy breach risks are high, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data (sensitive data).

DPIA's will help organisations identify potential privacy issues before they arise and come up with a solution to mitigate them. If the privacy issues cannot be mitigated then the organisation is required to consult their Data Protection Authority before engaging in the process. Ultimately a DPIA may prove invaluable in determining the viability of future projects and initiatives.

Organisations should therefore start to access the situations where it will be necessary to conduct a DPIA. If a DPIA is required to be undertaken the organisation needs to consider who will do it, who else needs to be involved and will the process run centrally or locally.

11). DATA PROTECTION OFFICERS (DPO)

It is important that someone in your organisation, or an external data protection advisor, takes responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

The appointment of a Data Protection Officer (DPO) will become mandatory for public organisations (except for courts acting in their judicial capacity), organisations that carry out the regular and systematic monitoring of individuals on a large scale, or organisations whose activities consist of processing sensitive personal data. The role of this DPO will be to support the organisations compliance with GDPR by ensuring personal data processes, activities, and systems conform by design. In addition, the DPO will act as an intermediary between the organisation and supervisory authorities or data subjects.

You should therefore consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet GDPR's requirements.

12). PROVISION OF 'ONE-STOP-SHOP'

Under the 'one-stop-shop' provision in GDPR, multinational organisations that have establishments in more than one EU member state, or have a single establishment in the EU that processes data of individuals in other EU states, will be allowed to deal with one Data Protection Authority as their single regulating body, referred to as a Lead Supervisory Authority (LSA).
The LSA will be in the country where the organisation has their main administration, or where decisions about data processing are made. The LSA will deal with all data protection matters involving that organisation and they will be obliged to consult other Data Protection Authorities in relation to certain matters.

Sources:

http://gdprandyou.ie/gdpr-12-steps/

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

*
"Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**
"Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

Damastown Way, Damastown Business Park, Dublin 15.

PH | 018227161 WB | www.grm.ie EM | info@grm.ie