GIBRALTAR REGULATORY AUTHORITY

Guidance on the General Data Protection Regulation: (1) Getting started

Guidance Note IR03/16

20th February 2017

Gibraltar Regulatory Authority
Information Rights Division
2nd Floor, Eurotowers 4, 1 Europort Road
Gibraltar
Telephone +350 20074636 Fax +350 20072166
Email: privacy@gra.gi
Web: http://www.gra.gi

Contents

Introduction into the General Data Protection Regulation

The General Data Protection Regulation (the "GDPR") will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

It is important to note that the UK's decision to leave the EU will not affect or influence the commencement of the GDPR in Gibraltar.

As an EU regulation, the GDPR will not generally require transposition (EU regulations have 'direct effect') and will automatically become law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority ("GRA"), as the Data Protection Commissioner, is aware that the increased obligations that the GDPR places on organisations might cause some anxieties for planners in the private sector as well as the public sector. This document is the first in a series that the GRA will issue in the run-up to the 25th May 2018 implementation date, to guide businesses and the public sector in preparing for compliance. The GRA's guidance will aim to complement other guidance produced by the Article 29 Working Party of EU data protection authorities at European level.

This initial guidance note provides a brief introduction into the GDPR and advises on the initial steps that organisations can take to get ready for the GDPR. In the guidance notes that will follow over the next few months, the GRA will provide more specific advice by focusing on specific areas of the GDPR, such as:

- Identifying a controller or processor's Lead Supervisory Authority;
- Data Protection Officers; and,
- Data Portability.

The GRA's objective is to alleviate some of the concerns for businesses and public sector organisations, and facilitate a smooth transition to future data protection standards for data controllers and data subjects alike.

Many of the main concepts and principles of the GDPR are much the same as those in our current Data Protection Act 2004 (the "DPA") so if you are compliant under the current law, then much of your approach should remain valid under the GDPR. However, the GDPR introduces new elements and significant enhancements which will require detailed consideration by all organisations involved in processing personal data. Some elements of the GDPR will be more relevant to certain organisations than others, and it is important and useful to identify and map out those areas which will have the greatest impact on your organisation.

It is essential that all organisations start preparing immediately for the implementation of the GDPR by carrying out a "review and enhance" analysis of all current or envisaged processing in line with the GDPR. This will allow time to ensure that you have adequate procedures in place to deal with the improved transparency, accountability and individuals' rights provisions, as well as optimising your approach to governance and how to manage data protection as a corporate issue. It is essential to start planning your approach to the GDPR compliance as early as you can, and to ensure a cohesive approach amongst key people in your organisation.

The sooner you begin to prepare for the GDPR, the more cost-effective it will be for your organisation. The GDPR gives data protection authorities more robust powers to tackle non-compliance, including significant administrative fining capabilities of up to €20,000,000 (around £18,000,000) (or 4% of total annual global turnover, whichever is greater) for the most serious infringements. The GDPR also makes it considerably easier for individuals to bring private claims against data controllers when their data privacy has been infringed, and allows data subjects who have suffered non-material damage as a result of an infringement to sue for compensation.

In order to provide clear guidance and a practical starting point, the GRA has compiled the following brief introduction into the GDPR, including advice on the initial steps that organisations can take to get ready for the GDPR.

1. Who does the GDPR apply to?

The GDPR applies to "data controllers" and "data processors". The definitions are broadly the same as under the DPA – i.e. the data controller is the organisation that says how and why personal data is processed and the data processor is the organisation that processes personal data on the data controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

2. What information does the GDPR apply to?

2.1. Personal data

Like the DPA, the GDPR applies to "personal data". However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. The change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

2.2. Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes. For example, the special categories specifically include genetic and biometric data, where processed to uniquely identify an individual.

3. What can I do NOW to prepare for the GDPR?

3.1. Becoming aware

It is imperative that key personnel in your organisation are aware that the law is changing to the GDPR, and start to factor this into their future planning. They should start to identify areas that could cause compliance problems under the GDPR.

Initially, data controllers should review and enhance their organisation's risk management processes, as implementing the GDPR could have significant implications for resources; especially for more complex organisations. Any delay in preparations may leave your organisation susceptible to compliance issues following the GDPR's introduction.

3.2. Becoming Accountable

Make an inventory of all personal data you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

3.3. Communicating with Staff and Service Users

Review all current data privacy notices alerting individuals to the collection of their data. Identify any gaps that exist between the level of data collection and processing your organisation engages in, and how aware you have made your customers, staff and services users of this fact. If gaps exist, set about redressing them using the criteria laid out under "Becoming Accountable" as your guide.

Before gathering any personal data, current legislation requires that you provide individuals with certain information such as your identity, your reasons for gathering the data, the use(s) it will be put to, who it will be disclosed to, and if it's going to be transferred outside the EU. Under the GDPR, additional information must be communicated to individuals in advance of processing, such as the legal basis for processing the data, retention periods, the right of complaint where individuals are unhappy with your implementation of any of these criteria, whether their data will be subject to automated decision making and their individual rights under the GDPR. The GDPR also requires that the information be provided in concise, easy to understand and clear language.

3.4. Personal Privacy Rights

You should review your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Rights for individuals under the GDPR include:

- Subject access
- To have inaccuracies corrected
- To have information erased
- To object to direct marketing
- To restrict the processing of their information, including automated decision-making
- Data portability

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA, but with some significant enhancements. Organisations who already apply these principles will find the transition to the GDPR less difficult.

Review your current procedures and ask yourselves the following questions:

- How would your organisation react if it received a request from a data subject wishing to exercise their rights under the GDPR?
- How long would it take you to locate (and correct or delete) the data from all locations where it is stored?
- Who will make the decisions about deletion?
- Can your systems respond to the data portability provision of the GDPR, if applicable where you have to provide the data electronically and in a commonly used format?

3.5. How will Access Requests change?

You should review and update your procedures and plan how you will handle requests within the new timescales. Currently, the DPA stipulates that a subject access request made under subsection 14 (3) must be complied with, by a data controller, within 28 days of receipt of the request. Under the GDPR there should be no undue delay in processing a subject access request and, at the latest, it must be concluded within one month.[1]

Under certain circumstances you will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The rules for dealing with subject access requests will change under the GDPR. You must provide a copy of the information free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request

1 As per article 12, subsection (3) of the GDPR, "The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay."

relates to. The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Organisations will have some grounds for refusing to grant an access request. Where a request is deemed manifestly unfounded or excessive, it can be refused. However, organisations will need to have clear refusal policies and procedures in place, and demonstrate why the request meets these 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. 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.

3.6. What we mean when we talk about a 'Legal Basis'

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it. This is particularly important where consent is relied upon as the sole legal basis for processing data. Under the GDPR, individuals will have a stronger right to have their data deleted where consent is the only justification for processing. You will have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request. Currently these are referred to as the "conditions for processing" under section 7 (1) of the DPA.

For government departments and agencies, there has been a significant reduction in the number of legal bases they may rely on when processing data. It will no longer be possible to cite legitimate interests. Instead, there will be a general necessity to have specific legislative provisions underpinning one or more of the methods organisations use to process data. All organisations need to carefully consider how much personal data they gather, and why. If any categories can be discontinued, do so. For the data that remains, consider whether it needs to be kept in its raw format, and how quickly you can begin the process of anonymization and pseudonymisation.

3.7. Using consent as grounds to process data

If you do use consent when you record personal data, you should review how you seek, obtain and record that consent, and whether you need to make any changes. Consent must be "freely given, specific, informed and unambiguous." Essentially, the individual cannot be forced into consent, or be unaware that

they are consenting to processing of their personal data. They must know exactly what they are consenting to, and there can be no doubt that they are consenting. Obtaining consent requires a positive indication of agreement – it cannot be inferred from silence, pre-ticked boxes or inactivity.

If consent is the legal basis relied upon to process personal data, you must make sure it will meet the standards required by the GDPR. If it does not, then you should amend your consent mechanisms or find an alternative legal basis. Note that consent has to be verifiable, that individuals must be informed in advance of their right to withdraw consent and that individuals generally have stronger rights where you rely on consent to process their data. The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail.

If you cannot reach this high standard of consent then you must find an alternative legal basis or cease or not start the processing in question.

3.8. Processing Children's Data

If the work of your organisation involves the processing of data from underage subjects, you must ensure that you have adequate systems in place to verify individual ages and gather consent from parents or guardians.

The GDPR introduces special protections for children's data, particularly in the context of social media and commercial internet services. The law will define the age up to which an organisation must obtain consent from a guardian before processing a child's data. It should be noted that consent needs to be verifiable, and therefore communicated to underage individuals in language they can understand.

Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

3.9. Reporting Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the GRA when they incur a personal data breach. However, the GDPR will bring in mandatory breach notifications, which will be new to many organisations. All breaches must be

reported to the GRA, typically within 72 hours, unless the data was anonymised or encrypted. In practice, this will mean that most data breaches must be reported to the GRA. Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned. Now is the time to assess the types of data you hold and document which ones fall within the notification requirement in the event of a breach. Larger organisations will need to develop policies and procedures for managing data breaches, both at central or local level.

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.

3.10. Data Protection Impact Assessments ("DPIA") and Data Protection by Design and Default

A DPIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow organisations to identify potential privacy issues before they arise, and come up with a way to mitigate them.

A DPIA can involve discussions with relevant parties/stakeholders. Ultimately, such an assessment may prove invaluable in determining the viability of future projects and initiatives. The GDPR introduces mandatory DPIAs for those organisations involved in high-risk processing; for example where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

Where the DPIA indicates that the risks identified in relation to the processing of personal data cannot be fully mitigated, data controllers will be required to consult the GRA before engaging in the process. Organisations should now start to assess whether future projects will require a DPIA and, if the project calls for a DPIA, consider:

- Who will do it?
- Who else needs to be involved?
- Will the process be run centrally or locally?

It has always been good practice to adopt privacy by design as a default approach; privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. However, the GDPR enshrines both the principle of 'privacy by design' and the principle of 'privacy

by default' in law. 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.

3.11. Data Protection Officers

The GDPR will require some organisations to designate a Data Protection Officer ("DPO"). Organisations requiring DPOs include public authorities, organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process what is currently known as sensitive personal data on a large scale.

The important thing is to make sure 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 do so effectively.

Therefore, you should 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 the GDPR's requirements.

3.12. International Organisations and the GDPR

The GDPR includes a 'one-stop-shop' provision which will assist those organisations which operate in many EU member states. Multinational organisations will be entitled to deal with one Data Protection Authority, referred to as a Lead Supervisory Authority ("LSA") as their single regulating body in the country where they are mainly established. That Data Protection Authority will then become the LSA when regulating all data protection matters involving that organisation, although it will be obliged to consult with other concerned Data Protection Authorities which are concerned in relation to certain matters.

In general, the main establishment of an organisation is determined according to where the organisation has its main administration, or where decisions about data processing are made. However, it would be helpful for you to map out where your organisation makes its most significant decisions about data processing, as this will help to determine your main establishment and therefore your LSA.

Important

This document is purely for guidance, and does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the GDPR will apply directly to them. The responsibility to become familiar with the Regulation and comply with its provisions from 25th May 2018 onwards therefore lies with the organisation. This guide is intended as a starting point only, and organisations may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific legal issues or queries.