The GDPR and You

General Data Protection Regulation

Preparing for 2018

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

The GDPR and You

General Data Protection Regulation

An Coimisinéir Cosanta Sonraí / Data Protection Commissioner

1

Becoming Aware

Review and enhance your organisation's risk management processes – identify problem areas now.

2

Becoming Accountable

Make an inventory of all personal data you hold. Why do you hold it? Do you still need it? Is it safe?

3

Communicating with Staff and Service Users

Review all your data privacy notices and make sure you keep service users fully informed about how you use their data.

4

Personal Privacy Rights

Ensure your procedures cover all the rights individuals are entitled to, including deletion and data portability.

5

How will Access Requests change?

Plan how you will handle requests within the new timescales – requests must be dealt with within one month.

6

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

Are you relying on consent, legitimate interests or a legal enactment to collect and process the data? Do you meet the standards of the GDPR?

7

Using Customer Consent as grounds to process data

Review how you seek, obtain and record consent, and whether you need to make any changes to be GDPR ready.

8

Processing Children's Data

Do do you have adequate systems in place to verify individual ages and gather consent from guardians?

9

Reporting Data Breaches

Are you ready for mandatory breach reporting? Make sure you have the procedures in place to detect, report and investigate a data breach.

10

Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default

Data privacy needs to be at the heart of all future projects.

11

Data Protection Officers

Will you be required to designate a DPO? Make sure that it's someone who has the knowledge, support and authority to do the job effectively.

12

International Organisations and the GDPR

The GDPR includes a 'one-stop-shop' provision which will assist those data controllers whose companies operate in many member states. Identify where your Main Establishment is located in the EU in order to identify your Lead Supervisory Authority.

Introduction

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

As a regulation, it will not generally require transposition into Irish law (regulations have 'direct effect'), so organisations involved in data processing of any sort need to be aware the regulation addresses them directly in terms of the obligations it imposes. 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 office of the Data Protection Commissioner (DPC) is aware that the increased obligations that the GDPR places on companies might cause some anxieties for business planners. This document is the first in a series that will issue in the run-up to the 25th May 2018 implementation date. The aim is to try to alleviate some of those concerns, and facilitate a smooth transition to future data privacy standards for data controllers and data subjects alike.

Many of the main concepts and principles of GDPR are much the same as those in our current Data Protection Acts 1988 and 2003 (the Acts) so if you are compliant under current law, then much of your approach should remain valid under the GDPR. However, GDPR introduces new elements and significant enhancements which will require detailed consideration by all organisations involved in processing personal data. Some elements of 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 business model.

It is essential that all organisations immediately start preparing for the implementation of GDPR by carrying out a "review and enhance" analysis of all current or envisaged processing in line with 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 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 (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.

Over the next few months the DPC will set out its plans to produce new guidance and other tools to assist in preparation for GDPR. In addition, the Article 29 Working Party of EU data protection authorities, of which the DPC is a member, will be producing guidance at European level. We will also be actively engaging with bodies representing the various industry sectors as part of our GDPR awareness campaign. It would be beneficial for your organisation to work closely with these bodies to share knowledge about implementation in your sector.

In order to provide clear guidance and a practical starting point, the DPC has compiled the following check list to assist you in your move towards 2018 and full compliance.

What can I do NOW to prepare for the GDPR?

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 organisations 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.

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. 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 in '2: Becoming Accountable' as your guide.

Before gathering any personal data, current legislation requires that you notify your customers of 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 customers 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.

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 Acts, but with some significant enhancements. Organisations who already apply these principles will find the transition to the GDPR less difficult.

Review your current procedures. How would your organisation react if it received a request from a data subject wishing to exercise their rights under the GDPR?

- How long 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?

5. How will Access Requests change?

You should review and update your procedures and plan how you will handle requests within the new timescales. (There should be no undue delay in processing an Access Request and, at the latest, they must be concluded within one month).

The rules for dealing with subject access requests will change under the GDPR. In most cases, you will not be able to charge for processing an access request, unless you can demonstrate that the cost will be excessive. The timescale for processing an access request will also shorten, dropping significantly from the current 40 day period.

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. 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. 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 customer 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.

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 anonymisation and pseudonymisation.

7. Using Customer Consent as grounds to process data

If you do use customer 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, your customer 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.

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 guardians.

The GDPR introduces special protections for children's data, particularly in the context of social media and commercial internet services. The state 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 your underage customers in language they can understand.

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 DPC 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 DPC, 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 DPC. 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 which 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.

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 oganisations 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 DPC 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.

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.

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 General Data Protection Regulation 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.