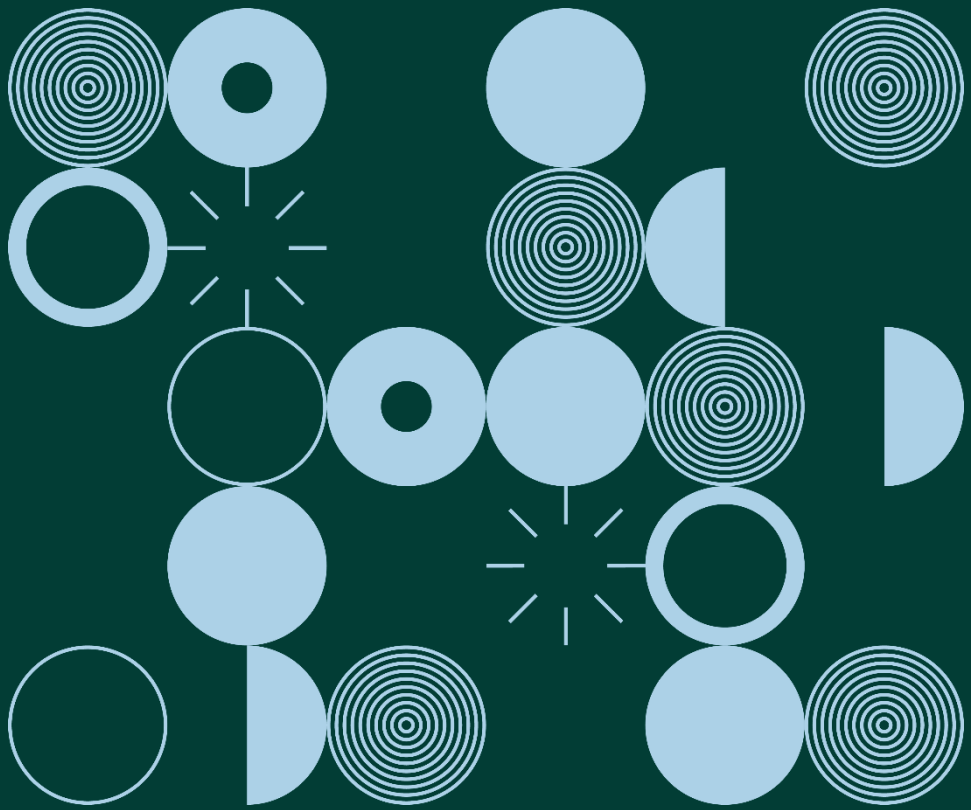
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

GDPR Guidance for SMEs

July 2019



SME READINESS CHECKLIST

What does the GDPR Mean for your Business/Organisation?

On the 25th May 2018, the General Data Protection Regulation (GDPR) came into effect across all EU member states. The GDPR provides one framework data protection law for Europe, representing a significant harmonisation of data protection requirements and standards across the EU. Having just one horizontal framework law to deal with will benefit business, promote responsibility when dealing with personal data, and help ensure that the same data protection standards apply across the EU.

However, despite being a direct-effect European Union Regulation, the GDPR provides some scope for EU Member States to implement further legislation to set national standards in some areas such as the processing of health data and criminal convictions, the digital age of consent and the circumstances in which an individual's data protection rights can be restricted. Accordingly, it is important for all businesses and organisations to be aware that they are required to comply with the data protection standards and obligations set out in both the GDPR and the Irish Data Protection Act 2018.

This guide and the accompanying checklist have been designed to assist in particular the small and medium enterprise (SME) sector, who may not have access to extensive planning and legal resources. Using this guide, along with our twelve-step GDPR and You guide, will help those businesses in particular to prepare for a business future that is data-protection compliant.

If you process personal data as part of your business, the GDPR applies to you. It is important to remember that:

- ✓ Customer AND employee data is personal data
- ✓ Simply storing personal data electronically or in hardcopy constitutes 'processing' personal data.

Key GDPR Definitions

GDPR: The General Data Protection Regulation (2016/679) is the new EU Regulation on Data Protection, which came into force on the 25th May 2018.

Personal Data: Information relating to a living individual who is, or can be, identified, including data that can be combined with other information to identify an individual. This can be a very wide definition, depending on the circumstances, and can include data which relates to the identity, characteristics or behaviour of an individual or influences the way in which that individual is treated or evaluated.

Processing: means performing any operation or set of operations on personal data, including:

- ✓ obtaining, recording or keeping data;
- ✓ organising or altering the data;
- ✓ retrieving, consulting or using the data;
- ✓ disclosing the data to a third party (including publication); and
- ✓ erasing or destroying the data.

Data Controller: A Data Controller is the person or organisation who decides the purposes for which, and the means by which, personal data is processed. The purpose of processing data involves 'why' the personal data is being processed and the 'means' of the processing involves 'how' the data is processed.

Data Processor: A person or organisation that processes personal data on behalf of a data controller.

Data Subject: A Data subject is the individual the personal data relates to.

Data Protection Impact Assessment (DPIA): A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the GDPR.

Legal Basis for Processing: In order to process personal data you must have a legal basis to do so. The legal bases (or justifications) for processing personal data are set out in Article 6 GDPR. These are the consent of the individual or where it is necessary for: performance of a contract; compliance with a legal obligation; protection the vital interests of a person; the performance of a task carried out in the public interest; or in pursuit of the legitimate interests of the company/organisation or another (except where those interests are overridden by the interests or rights and freedoms of the data subject).

Retention Policy: How long will your organisation hold an individual's personal data? This will be influenced by a number of factors. There may be legal requirements on your organisation, depending on your business type (e.g. medical council rules). Keep the data for the least amount of time that you can in accordance with the requirements of your business, store it securely while it is in your possession and make sure to delete it fully and safely at the appointed time.

Special Categories (sensitive) of Personal Data: This is defined in Article 9(1) GDPR as data which reveals 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. Processing such data is not permitted unless one or more of the conditions in Article 9(2) GDPR are met. Where this requirement is met, controllers also require a legal basis under Article 6 to justify the processing of special category personal data.

Consent: Article 7 GDPR has strengthened the conditions needed for consent as a legal basis for data processing to be valid. It is necessary to consider whether consent was freely given and the data subject must have the opportunity to withdraw consent for processing at any time. Consent should not be assumed and must be obtained before data processing begins.

The Key Steps to Take to Ensure GDPR Compliance

- ✓ Identify what personal data you hold (this can be achieved by setting out the information listed in Article 30 GDPR or for smaller companies a tailored process such as the accompanying template that identifies details of personal data held).
- ✓ Conduct a risk assessment of the personal data you hold and your data processing activities (Article 24, Recital 75 and section titled "Risk based approach to being GDPR compliant").
- ✓ Implement appropriate technical and organisational measures to ensure data (on digital and paper files) is stored securely. The security measures your business should put in place will depend on the type of personal data you hold and the risk to your customers and employees should your security measures be compromised (Article 32).
- ✓ Know the legal basis you rely on (consent? contract? legitimate interest? legal obligation?) to justify your processing of personal data (Articles 6 to 8).
- ✓ Ensure that you are only collecting the minimum amount of personal data necessary to conduct your business, and the data are accurate and kept no longer than is needed for the purpose for which they were collected (Article 5).
- ✓ Be transparent with your customers about the reasons for collecting their personal data, the specific uses they will be put to, and how long you need to keep their data on file (e.g. notices on your website or signs at points of sale) (Articles 12, 13 and 14).
- ✓ Establish whether or not the personal data you process falls under the category of special categories (sensitive) of personal data and, if it does, know what additional precautions you need to take (Article 9).
- ✓ Decide whether you will need to retain the services of a Data Protection Officer (DPO) (Article 37).
- ✓ Be able to facilitate requests from service users wishing to exercise their rights under the GDPR, including rights of access, rectification, erasure, withdrawal of consent, data portability and the right to object to automated processing (Articles 12 to 22).
- ✓ Have up-to-date policy documents and/or internal procedures.

A Risk-Based Approach to Being GDPR Compliant

When your organisation collects, stores or uses (i.e. processes) personal data, the individuals whose data you are processing may be exposed to risks. It is important that organisations which process personal data take steps to ensure that the data is handled legally, securely, efficiently and effectively in order to deliver the best possible care.

The risk-profile of the personal data your organisation processes should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed. For example, where a data processing activity is particularly complex, or where a large volume or sensitive data is involved (i.e. an internet, health, financial or insurance company), this would attract a higher risk rating than routine personal data that relates solely to employee or customer account details.

When looking at the risk profile of the personal data your organisation processes, it is useful to look at the tangible harm to individuals that your organisation needs to safeguard against. These are detailed in Recital 75 GDPR and include processing that could give rise to: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation; or any other significant economic or social disadvantage.

Conducting a risk assessment will improve awareness in your organisation of the potential future data protection issues associated with a project. This will in turn help to improve the design of your project and enhance your communication about data privacy risks with relevant stakeholders.

The GDPR provides for two crucial concepts for future project planning: **Data Protection by Design** and **Data Protection by Default.** While long recommended as good practice, both of these principles are enshrined in law under the GDPR (Article 25).

Data Protection by Design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Protection by Default means that the user service settings must be automatically data protection friendly (e.g. avoid automatic opt-ins on customer privacy settings), and that only data which is necessary for each specific purpose of the processing should be gathered and otherwise processed in the first place.

Under the GDPR, a Data Protection Impact Assessment (DPIA) is a mandatory pre-processing requirement where the envisaged project/initiative/service involves data processing which *"is likely to effect in a high risk to the rights and freedoms of natural persons*." This is particularly relevant when a new data processing technology is being introduced in your organisation. In cases where it is not clear whether a DPIA is strictly

mandatory, carrying out a DPIA may still be the best approach and a very useful tool to help data controllers demonstrate their compliance with data protection law. DPIAs are scalable and can take different forms, but the GDPR sets out the basic requirement of an effective DPIA.

Maintaining a data protection risk register can allow you to identify and mitigate against data protection risks, as well as demonstrate compliance in the event of a regulatory investigation or audit.

GDPR Readiness Checklist Tools:

In addition to the general checklist below, the following pages will take organisations through more detailed questions in the areas of:

- ✓ personal data
- ✓ data subject rights
- ✓ accuracy and retention
- ✓ transparency requirements
- ✓ other data controller obligations
- ✓ data security
- ✓ data breaches
- ✓ international data transfers

The following grid will assist organisations in mapping the personal data that they currently hold and process, the lawful basis on which the data was collected, and the retention period for each category of data. Carrying out this exercise will help identify where immediate remedial actions are required in order to be compliant with the GDPR.

Categories of personal data and data subjects	**Elements of personal data included within each data category**	**Source of the personal data**	**Purposes for which personal data is processed**	**Legal basis for each processing purpose**	**Special categories of personal data**	**Basis for processing special categories of personal data**	**Retention period**	**Action required to be GDPR compliant?**
List the categories of data subjects and personal data collected and retained e.g. current employee data; retired employee data; customer data (sales information); marketing database; CCTV footage.	List each type of personal data included within each category of personal data e.g. name, address, banking details, purchasing history, online browsing history, video and images.	List the source(s) of the personal data e.g. collected directly from individuals; from third parties (if a third party identifies the data controller as this information will be necessary to meet obligations under Article 14).	Within each category of personal data list the purposes for which the data is collected and retained e.g. marketing, service enhancement, research, product development, systems integrity, HR matters, advertising.	For each purpose that personal data is processed, list the legal basis on which it is based e.g. consent, contract, legal obligation (Article 6).	If special categories of personal data are collected and retained, set out details of the nature of the data e.g. health, genetic, biometric data.	List the legal basis on which special categories of personal data are collected and retained e.g. explicit consent, legislative basis (Article 9).	For each category of personal data, list the period for which the data will be retained e.g. one month? one year? As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.	Identify actions that are required to ensure all personal data processing operations are GDPR compliant e.g. this may include deleting data where there is no further purpose for retention

Personal Data

	Question	Yes	No	Comments/ Remedial Action
Processing personal data based on consent (Articles 7, 8 and 9)	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of a statement or a clear affirmative action?			
	If personal data were held on the basis of consent does it meet the required standard under the GDPR, or have you re-sought the individual's consent to ensure compliance with the GDPR where necessary?			
	Are procedures in place to demonstrate that an individual has consented to their data being processed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
Processing children's personal data (Article 8)	Where online services are provided to a child, are procedures in place to verify age and get consent from a parent/ legal guardian, where required?			
Processing personal data based on legitimate interests	If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? (That analysis must demonstrate that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, and 3) the processing is not prejudicial to or overridden by the rights of the individual)			

Data Subject Rights

	Question	Yes	No	Comments/ Remedial Action
Access to personal data (Article 15)	Is there a documented policy/procedure for handling Subject Access Requests (SARs)?			
	Is your organisation able to respond to SARs within one month?			
Data portability (Article 20)	Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format?			
Deletion and rectification (Articles 16 and 17)	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
Right to restriction of processing (Article 18)	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
Right to object to processing (Article 21)	Are individuals told about their right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest?			
	Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
Profiling and automated processing (Article 22)	If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected?			
	Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?			
Restrictions to data subject rights (Article 23)	Have the circumstances been documented in which an individual's data protection rights may be lawfully restricted?			

Accuracy and Retention

	Question	Yes	No	Comments/ Remedial Action
Purpose Limitation	Are personal data only used for the purposes for which they were originally collected?			
Data minimisation	Are the personal data collected limited to what is necessary for the purposes for which they are processed?			
Accuracy	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Retention	Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?			
Other Legal Obligations Governing Retention	Is your business subject to other rules that require a minimum retention period (e.g. medical records/tax records)?			
	Do you have procedures in place to ensure data are destroyed securely, in accordance with your retention policies?			
Duplication of Records	Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records?			

Transparency Requirements

	Question	Yes	No	Comments/ Remedial Action
Transparency to customers and employees (Articles 12, 13 and 14)	Are service users/employees fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language?			
	Where personal data are collected directly from the individuals, are procedures in place to provide the information listed at Article 13 of the GDPR?			
	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
	If personal data are not collected from the subject but from a third party (e.g. acquired as part of a merger) are procedures in place to provide the information listed at Article 14 of the GDPR?			
	When engaging with individuals, such as when providing a service, sale of a good or CCTV monitoring, are procedures in place to proactively inform individuals of their GDPR rights?			
	Is information on how the organisation facilitates individuals exercising their GDPR rights published in an easily accessible and readable format?			

Other Data Controller Obligations

	Question	Yes	No	Comments/ Remedial Action
Supplier Agreements (Articles 27 to 29)	Have agreements with suppliers and other third parties processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included?			
Data Protection Officers (DPOs) (Articles 37 to 39)	Do you need to appoint a DPO as per Article 37 of the GDPR?			
	If it is decided that a DPO is not required, have you documented the reasons why?			
	Where a DPO is appointed, are escalation and reporting lines in place? Are these procedures documented?			
	Have you published the contact details of your DPO to facilitate your customers/ employees in making contact with them?			
	Have you notified your data protection authority (such as the DPC) of your DPO's contact details?			
Data Protection Impact Assessments (DPIAs) (Article 35)	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			

Data Security

	Question	Yes	No	Comments/ Remedial Action
Appropriate technical and organisational security measures (Article 32)	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
Documented security programme	Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative and physical safeguards for personal data?			
	Is there a designated individual who is responsible for preventing and investigating security breaches?			
	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
	Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			

Data Breaches

	Question	Yes	No	Comments/ Remedial Action
Data Breach Response Obligations (Article 33 and 34)	Does the organisation have a documented privacy and security incident response plan?			
	Are there procedures in place to notify the Data Protection Commission of a data breach?			
	Are there procedures in place to notify data subjects of a data breach (where applicable)?			
	Are plans and procedures regularly reviewed?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches?			

International Data Transfers (outside EEA) (if applicable)

	Question	Yes	No	Comments/ Remedial Action
International Data Transfers (Articles 44 to 50)	Are personal data transferred outside the EEA, e.g. to the US or other countries?			
	Does this include any special categories of personal data?			
	What is the purpose(s) of the transfer?			
	Who is the transfer to?			
	Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data are exported and which country receives the data and who the recipient of the transfer is?)			
Legality of International Transfers	Is there a legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses. Are these bases documented?			
Transparency	Are data subjects fully informed about any intended international transfers of their personal data?			