The GDPR Readiness Checklist

The following checklist will help you prepare and evaluate the readiness of your organisation for the General Data Protection Regulation (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 (nonspecial categories of personal data)	Special categories of personal data	Legal 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 third party identify 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 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.*

Co-funded by the Erasmus+ Programme of the European Union

Personal Data

	Question	Yes	No	Comment/Remedial Action
Consent based data processing (Articles 7, 8 and 9 and further guidance available on GDPRandYou.ie)	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 statement or a clear affirmative action?			
	If personal data that you currently hold on the basis of consent does not meet the required standard under the GDPR, have you re-sought the individual's consent to ensure compliance with the GDPR?			
	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?			
Children's personal data (Article 8)	Where online services are provided to a child, are procedures in place to verify age and get consent of a parent/ legal guardian, where required?			
Legitimate interest based data processing	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.			

Co-funded by the Erasmus+ Programme of the European Union

Data Subject Rights

	Question	Yes	No	Comment/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 and further guidance available on GDPRandYou.ie)	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?			

Co-funded by the Erasmus+ Programme of the European Union

	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 and further guidance available on GDPRandYou.ie)	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? Note: the Irish Data Protection Bill will set out further details on the implementation of Article 23.			

Co-funded by the Erasmus+ Programme of the European Union

Accuracy and Retention

	Question	Yes	No	Comment/Remedial Action
Purpose limitation	Is personal data only used for the purposes for which it was originally collected?			
Data minimisation	Is the personal data collected limited to what is necessary for the purposes for which it is processed?			
Accuracy	Are procedures in place to ensure personal data is 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 is held for no longer than is necessary for the purposes for which it was 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 is 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?			

Co-funded by the Erasmus+ Programme of the European Union

Transparency Requirements

	Question	Yes	No	Comment/Remedial Action
Transparency to customers and employees (Articles 12, 13 and 14 and further guidance available on GDPRandYou.ie)	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 is collected directly from the individuals, are procedures in place to provide the information listed at Article 13 of the GDPR?			
	If personal data is 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?			

Co-funded by the Erasmus+ Programme of the European Union

Other Data Controller Obligations

	Question	Yes	No	Comment/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 and further guidance available on GDPRandYou.ie)	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? (Note: post 25 May 2018 you will also be required to notify your data protection authority of your DPO's contact details)			

Co-funded by the Erasmus+ Programme of the European Union

Data Protection Impact Assessments (DPIAs) (Article 35 and further guidance available on GDPRandYou.ie)	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?			

Co-funded by the Erasmus+ Programme of the European Union

Data Security

	Question	Yes	No	Comment/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?			
	Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?			
	Is there a documented process for resolving security related complaints and issues?			
	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?			
	Is personal information systematically destroyed, erased, or anonymised when it is 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?			

Co-funded by the Erasmus+ Programme of the European Union

Data Breaches

	Question	Yes	No	Comment/Remedial Action
Data Breach response obligations (Article 33 and 34 and further guidance available on GDPRandYou.ie)	Does the organisation have a documented privacy and security incident response plan?			
	Are plans and procedures regularly reviewed?			
	Are there procedures in place to notify the office of the Data Protection Commissioner of a data breach?			
	Are there procedures in place to notify data subjects of a data breach (where applicable)?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches?			

Co-funded by the Erasmus+ Programme of the European Union

International Data Transfers (outside EEA) – *if applicable*

	Question	Yes	No	Comment/Remedial Action
International data transfers (Articles 44 to 50)	Is 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 is 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?			

Co-funded by the Erasmus+ Programme of the European Union

Based on Data Protection Commissioner: www.dataprotection.ie

Co-funded by the
Erasmus+ Programme
of the European Union