Data Protection and GDPR Refresher

Prepared for

Irish Tax Institute

Ronan Daly Jermyn

Disclaimer: This document is intended for general guidance only and does not constitute legal advice. Independent legal advice should be sought prior to relying on anything within this document.

Responding to a Data Breach

Given the potentially significant impact of security breaches on both data subjects and associated reputational damage for companies, it is unsurprising that data security has received a significant amount of attention in the GDPR.

In responding to a data breach, organisations should consider:

- Notification to Supervisory Authority: Currently, there is no requirement to notify the Data Protection Commissioner (DPC) of a data breach, although the current Data Security Breach Code of Practice recommends the reporting of such breaches. GDPR requires that where there is a risk to the "rights and freedoms" of individuals, controllers are obliged to notify the DPC of the breach. After becoming aware of the breach, the controller is required, without undue delay (within 72 hours where feasible), to notify the personal data breach.

- Notification to Data Subjects: Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to notify the data subject of the personal data breach without undue delay.

- Processor to Controller Notification: Upon becoming aware of a data breach, processors are required to notify controllers without undue delay.

- Notification to Insurers and Legal Advisors: Controllers should notify their insurers of a data breach and also consider reviewing polices now to ensure they are covered for cyber-attacks. Legal advice should be sought at an early stage.

- Maintaining Records: Organisations are required to maintain a record of any personal data breaches so as to enable the DPC to verify compliance with the controller's notification requirements. Records must demonstrate the facts relating to the data breach, its effects and the remedial action taken.

- Policies: Organisations should prepare draft template security breach notifications and security breach plans so as to be in the best position to act quickly should a breach occur.

Information for Privacy Notices

The EU General Data Protection Regulation (GDPR) rules on giving privacy information to data subjects are contained in Articles 12, 13 and 14. These are more detailed and specific than, for example, in the Irish Data Protection Acts and place an emphasis on making privacy notices more transparent, and accessible.

A privacy notice must be supplied to the individual at the time they provide the Company with their personal data. The GDPR states that the information you provide to people about how you process their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The types of information that must be included in a privacy notice pursuant to Article 12, where the data subject is providing you with their data, are as follows:

a. Identity and contact details of the Data Controller.

'Data Controller' is defined under GDPR as the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data, in this case, this will be the Company, but may also be for example your pension provider.

b. Contact details of the Data Protection Officer, where applicable.

The requirement to appoint a DPO will apply to:

1. companies whose core activities consist of:
   a. data processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale; or
   b. processing on a large scale of the special categories of data and data relating to criminal convictions; and
2. all public bodies and authorities (other than courts acting in their judicial capacity).

In addition, EU member states may specify other circumstances in which the appointment of a DPO will be mandatory within that EU member state.

c. What information does the Company collect about the individual?

Outline the types of personal data being processed. The GDPR defines personal data as the following:

'Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'

Personal data relating to employee can include: name, job title, date of birth, passport data, home address, home telephone number, pps number, private email address, emergency contact, staff number etc.

'Special categories' of personal data (sensitive personal data) relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special category data relating to employee can include: racial and ethnic origin, religion, health records etc.

d. How will the individual's information be used?

Outline the purposes for the processing. Processing essentially means undertaking any action involving personal data.

e. What is the Company's legal basis for processing personal data?

For processing to be lawful under the GDPR, the Company needs to identify a lawful basis before it can process personal data. It is important that you determine your lawful basis for processing personal data and document this.

If you are processing personal data then you must satisfy a condition under Article 6 and if you are processing special category data then you must satisfy a condition under Article 6 and Article 9.

Article 6 - Personal Data	Article 9 - Special Categories
The data subject has given ***consent*** to the processing *	The data subject has given ***explicit consent*** to the processing
Processing is necessary for the performance of a ***contract*** with the data subject	Processing is necessary for the purposes of carrying out the obligations of the controller or of the data subject in the field of ***employment***
Processing is necessary for compliance with a ***legal obligation***	Processing is necessary to protect the ***vital interests*** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
Processing is necessary in order to protect the ***vital interests*** of the data subject or of another natural person	Processing is carried out in the course of its legitimate activities by a foundation, association or any other ***not-***

	for-profit body with a political, philosophical, religious or trade union aim.
Processing is necessary for the performance of a task carried out in the *public interest*	Processing relates to personal data which are made *public* by the data subject
Processing is necessary for the purposes of the *legitimate interests* pursued by the controller or by a third party.**	Processing is necessary for the establishment, exercise or defence of *legal claims* or whenever courts are acting in their judicial capacity
	Processing is necessary for reasons of *substantial public interest*
	Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of *health or social care* or treatment, or the management of health or social care systems
	Processing is necessary for reasons of public interest in the area of *public health*
	Processing is necessary for *archiving purposes* in the public interest, scientific or historical research purposes or statistical purposes

*Rules around consent are much stricter under GDPR. Consent means offering individuals genuine choice and control and requires a positive opt-in. Pre-ticked boxes and any other methods of consent by default are not lawful. The GDPR gives individuals a specific right to withdraw consent. You need to tell individuals about their right to withdraw, and offer them easy ways to withdraw consent at any time

**In order to rely on the 'legitimate interests' condition you must meet certain requirements. The first requirement is that you must need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

f. Who receives your information?

Here you will need to specify the recipients or categories of recipients of data. Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

g. Any transfers to third countries and the safeguards in place

Here you will need to specify if the data will be transferred outside of the EU and how this transfer is justified.

h. How long will information be held?

Here you will need to specify the retention period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. It is important to be aware that the GDPR states that personal data must be kept 'no longer than is necessary for the purposes'. Please see the separate document on retention periods provided for further information on statutory retention periods.

i. What are the individual's rights?

Here you will need to inform data subjects about their rights under the GDPR including their rights to access and port data, to rectify, erase and restrict his or her data, to object to processing as well as the right to withdraw consent if processing is based on consent. Individuals have a right to access their personal information, to object to the processing of their personal information, to rectify, to erase, to restrict and to port their personal information.

j. Security of information

Here you will need to provide some information on how the data will be kept secure.

k. How a complaint is made

If an individual is unhappy with the way in which their personal data has been processed, they need to be told how that can be addressed. They also need to be told that they have the right to lodge a complaint with their national supervisory authority.

Retention Periods

When developing a policy on retention of HR records, the Company must have regard to specific pieces of employment legislation and the Data Protection Acts, 1988 and 2003 ("the DPA"). The latter requires that personal data is retained "for no longer than is necessary" for the purpose or purposes for which it was obtained. This principle is unchanged by GDPR, however it enhances the existing provisions set out in the DPA and has also introduced a new requirement for data controllers to be able to demonstrate compliance with GDPR as discussed earlier.

Of note, Article 30, GDPR, provides for record keeping and obliges data controllers, where possible, to set out the envisaged time limits for erasure of the different categories of data. Employers, as data controllers, must be clear about the length of time for which employment records comprising of personal and sensitive personal data relating to their employees, are retained and also why that information is being retained.

Coupled with this requirement, certain employment legislation prescribe a statutory minimum period to retain records and these statutory obligations constitute a lawful basis for the mention of those records, such as to be compliant with the DPA and GDPR.

The following statutory obligations apply to employers in relation to retention of employment records:

Legislation	Retention Period	Data
The Terms of Employment (Information) Act, 1994	the duration of their employment	employee's terms and conditions of employment
The National Minimum Wage Act, 2000	3 year retention period to show compliance with the Act's provisions	payslips showing the employees were paid at least minimum wage
The Organisation of Working Time Act, 1997 and the Organisation of Working Time (Records) Prescribed Form and Exemptions) Regulations 2001	3 year retention period	records of weekly working hours, the name and address of employee, the employee's PPS numbers and a statement of their duties
The Protection of Young Persons (Employment) Act, 1996	3 year retention period	employment records relating to persons under 18 years of age
The Protection of Employment Acts, 1977-2007	3 year retention period	where an employer has collective redundancies, it must retain the records to show that the provisions of the Act were complied with
The Parental Leave Acts 1998-2006	8 year retention period	records showing the dates and times an employee availed of parental or force majeure leave

The Companies Acts and Taxes Consolidation Act, 1997	6 year retention period	tax records
The Safety, Health and Welfare at Work (General Applications) Regulations 1993	10 year retention period	Details of workplace accidents

It is clear that retention of employment records involves a balancing exercise between data protection principles on the one hand and the employment legislative requirements set out above, on the other. It is important for you to ascertain on what basis you are retaining records.

Where an employer believes that records may be required to defend litigation that has been threatened or commenced, then those records should be retained in order to assist in the defence of those proceedings. Records should not be retained indefinitely on the chance that proceeding may be issued, but rather where there is a high risk. The most common applicable records would be concerning personal injuries or actions for breach of contract.

The retention period in these cases are determined by the relevant limitation period set out in the Statute of Limitations, 1957:

Legislation	Retention Period	Data
Personal injuries - Statute of Limitations 1957	2 years from date of cause of action and a period of 3 years is the general recommended retention period to allow time for proceedings to be served	Data relating to the injury
Breach of Contract - Statute of Limitations 1957	6 years from the date of breach	Contracts should be retained for a period of at least 7 years from the date of termination of the employment, again to allow for proceedings to be served
Employment Equality Acts, 1998 to 2015	1 year period	records relating to a recruitment process