MASON
HAYES &
CURRAN

Pension Trustees

Final Countdown to the GDPR

Introduction

The General Data Protection Regulation (GDPR) will come into force in all EU Member States in May 2018. It is not a radical departure from the current Irish data protection regime under the Data Protection Acts 1988 and 2003 (DPA), rather it has built on existing concepts and requirements and added new obligations. Its purpose is to beef up protections, compliance requirements and sanctions to reflect modern data processing practices.

All pension trustees, sponsoring employers, administrators and service providers will be affected by this change in law and should currently be preparing for this. As a data controller, pension trustees should be assessing their current data protection practices and identifying compliance gaps that will need to be filled before the GDPR comes into effect in May.

The GDPR brings with it a significant increase in the sanctions for noncompliance. Companies can be fined up to €20,000,000 or 4% of annual global turnover, whichever is higher.

We review the data protection concepts, key changes for pension trustees and recommended steps towards compliance.

Key Concepts

Data protection is the means by which the rights of individuals, known as **data subjects**, are protected in relation to the processing of their personal data.

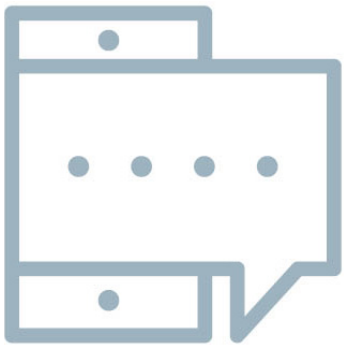
Personal data is broadly defined under current law, and even more so under the GDPR, so as to cover any information relating to an identified/identifiable living person. Article 4 of the GDPR gives non-exhaustive examples of information that could identify a person and these include: name; identification number; location data; online identifiers including IP addresses and cookies; and the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

Generally, the person or corporate body who decides how personal data is collected from data subjects, why it is collected and how it is used, is known as a **data controller**. A data controller is primarily responsible for the personal data it controls and must ensure all uses are in compliance with applicable data protection law.

Most will be familiar with the term "**process**" or "**processing**" in the context of data protection. This is the legal term given for the uses of, and activities performed on, personal data. Processing, under data protection law, is a very broad term which covers activities such as the collection, storage, retrieval, consultation, use, sharing and erasure of personal data.

Data controllers often need the assistance of third parties to carry out certain tasks which may involve the processing of personal data.

These third parties, to the extent they process personal data on behalf of the data controller, are known as **data processors**.



Pension Trustees are Controllers of Member Data

All pension trustees handle personal data to varying degrees. If a trustee decides how members' personal data is collected and processed, it is deemed to be a data controller under the EU data protection regime.

Therefore, that pension trustee is responsible for compliance with the applicable data protection laws.

A pension trustee generally controls and processes scheme members' non-sensitive personal data, such as their name, address, date of birth, job title, salary, etc. A pension trustee might also control information which directly or indirectly relates to a member's physical or mental health. This health related information is categorised as sensitive personal data and carries with it heightened obligations under data protection law.

What are the Key Changes for Irish Pension Trustees?

Accountability

One of the biggest changes for pension trustees will be the new compliance obligations introduced by the GDPR under the 'accountability' principle.

This requires pension trustees, as the data controller, and any data processors engaged by pension trustees, to be able to show how they comply with their data protection obligations.

- *Record Keeping*: Trustees will have to keep up to date written records (electronic form is permitted) of their data processing activities including: (i) the purpose of the processing; (ii) a description of the categories of personal data and data subjects; (iii) the categories of recipients to whom the personal data is or may be disclosed; (iv) details of transfers of personal data outside of the European Economic Area; (v) where possible, the envisaged periods of retention of the different categories of data; and (vi) where possible, a general description of the technical and organisational security measures in place. These records must be made available to the Data Protection Commissioner's Office (DPC), if requested.
- *Privacy Impact Assessments (PIA)*: The GDPR requires controllers, but not processors, to carry out documented impact assessments for high-risk processing. The aim of PIAs is to assess the need for, and potential benefit of, the processing against the impact on the relevant data subjects. If, for example, a pension trustee intends to implement a new technology or policy which carries risks for members' personal data, it may need to carry out a PIA in advance to assess the severity of those risks. If a data protection officer is appointed, he/she must be involved in the assessment.
- *Data Protection Officer (DPO)*:A significant new obligation under the GDPR is the requirement for certain types of companies, whether acting as controllers or processors, to appoint a DPO. Many pension schemes' circumstances are unlikely to trigger the requirement for a mandatory appointment of a DPO. If a trustee is not required to appoint a DPO, careful consideration should be taken before voluntarily designating a person as a DPO. Voluntary appointments attract the same stringent GDPR requirements as a mandatory appointment. Therefore, if trustees wish to avoid being considered as having appointed a DPO it should ensure that the person's role, job specification and title do not suggest a voluntary appointment was made.

Consent

Under the DPA and GDPR, a data controller must have a valid legal basis for processing personal data. Typically, under the DPA, controllers relied on persons' implied consent, e.g. a browse-wrap privacy policy, to process non-sensitive personal data and explicit consent (e.g. signing a privacy policy) if any sensitive personal data is processed.

However, the GDPR raises the bar on what is required in order to obtain a person's valid consent. This means a data controller must ensure that:

- the data subject's consent is freely given
- the person is fully informed of what they are consenting to before consent is given
- the consent is obtained by way of a clear affirmative action. Silence is insufficient.
- separate consents must be given for separate purposes
- consent can be refused
- a person must be able to withdraw their consent at any time. They must be informed of this right from the outset as part of the notice requirements

If pension trustees currently rely on members' consent to process their personal data, it is very likely that those consents will not meet the standards required under the GDPR. Therefore, either fresh, GDPR compliant consents should be sought from members as soon as possible or another legal justification for processing member data should be identified, such as legitimate interest, legal obligation or contractual necessity.

The legal bases for processing sensitive personal data, such as medical information, are different and more restricted than the basis a controller can rely on to process nonsensitive data. Pension trustees may continue to rely on members' explicit consent to process their sensitive personal data, but will need to review this process against the consent standards under the GDPR.

Other Legal Grounds

Reliance on members' consent to process non-sensitive data may no longer be practical for pension trustees, primarily because members can refuse to give their consent or withdraw it at any time. As a result, trustees should consider other legal bases, which may warrant the processing of member data. The following legal bases would appear to be most relevant for trustees:

- Necessary for the performance of a contract to which the member is a party
- Necessary for compliance with a legal obligation to which the trustee is subject
- Necessary for the purposes of the legitimate interests pursued by the trustee

Trustees will need to assess the legal grounds on which its data processing activities are to be carried out under the GDPR, and both justify that basis and record their thinking (i.e. under the 'accountability' principle).

When relying on legitimate interest, the processing must be necessary for those legitimate interests and the members' interests or fundamental rights and freedoms must be taken into account. In addition, legitimate interest is not a valid legal basis for processing sensitive personal data. Therefore, pension trustees may need to rely on explicit member consent or some other legal justification available under Article 9(2) of the GDPR if it needs to handle members' health data.

Privacy Notices

Trustees, as data controllers, are obliged to process personal data fairly and lawfully 'in a transparent manner'. As part of this obligation, the GDPR requires that certain minimum information be given to individuals. This information may be presented in a privacy notice or policy. The notice must be clearly accessible and available at the time members' personal data is collected.

Article 13(1) of the GDPR lists information that must be contained in a privacy notice, which includes:

- identity and contact details of the controller and DPO, if one is appointed
- the purpose for processing the data
- the legal basis for the processing
- details of third parties to whom the data may be disclosed
- details (including the legal basis) of transfers of the data outside of the EEA

Other information that may need to be given, if appropriate, include:

- data retention periods
- the data subjects' rights which include rights of access, rectification, restriction, erasure, objection and portability
- the right to withdraw consent, if consent is relied upon to process data

The task of providing this level of detail 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language' will be challenging for pension trustees.

Service Providers

Trustees typically engage third parties to perform certain services for a pension scheme. These third parties can include external administrators, actuaries, investment advisors, IT services, etc. If any of these suppliers handle members' personal data, they will likely be deemed a data processor under the DPA and the GDPR.

Under the GDPR, these data processors will be subject to direct legal obligations. However, data controllers such as pension trustees are not relieved of their obligations under the GDPR, even if they have delegated certain tasks to a third party data processor.

Whilst the DPA currently obliges data controllers to have contracts with third parties that process personal data on their behalf, it specifies very little on the content of those contracts. However, the GDPR is very different in this regard. The new regime expressly requires that a number of clauses be included in a processing contract between the data controller and the data processor. These clauses include obligations relating to data transfers outside of the EEA, confidentiality, data security, sub-processing, security breach notification and deletion.

The GDPR provides for joint and several liabilities between data controllers and processors. Therefore, it is important that contracts contain an appropriate apportionment clause and indemnities to protect a party from being left out of pocket as a result of damage caused by a contracting party, and to provide for dispute resolution mechanisms.

Security Incidents

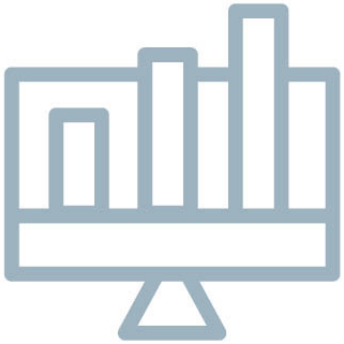
Currently, a data controller or processor regulated by the DPA is not specifically obliged by the DPA to report a data breach to the affected data subjects or to the DPC. However, the Personal Data Security Breach Code of Practice (Code) published by the DPC, whilst not legally binding on controllers or processors, should always be considered when a personal data security breach is identified.

One of the new introductions of the GDPR is a uniform breach notification rule across the EU. Whilst in practice the notification requirements under the GDPR may not be as strict as the Code, controllers and processors will be required by law to comply with these obligations. Non-compliance may result in heavy fines. This is a considerable deviation from the position under the Code.

GDPR is Less Than Five Months Away - What Trustees Need to Do

The following are just some of the steps pension trustees should be implementing now, or as soon as possible in advance of 25 May 2018:

- *Internal audit*: Identify what personal data you hold, why you hold it, where it is stored and how long you retain it. Also identify who and where you transfer it to.
- *Gap analysis*: In addition to the data audit, carry out a gap analysis of your existing data protection control environment against the GDPR requirements. For example, if you rely on consent, you will likely need to obtain new consents that comply with the GDPR. Due to the heightened requirements for valid consent, you may need to consider another legal basis such as legitimate interest to process some or all member data.
- *Privacy notices*: Whatever legal basis you rely on to process members' personal data, the privacy statements currently used will likely need a refresh. They should include all information designated as mandatory under the GDPR, yet deliver on the obligation for these notices to be concise and in clear and plain language.
- *Accountability*: Are you obliged to appoint a DPO, or will you voluntarily designate someone to be responsible for compliance? Processes will need to be implemented to satisfy the new record keeping obligations. Also, new internal policies should be developed and put in place to deal with security, detection and management of data breaches, use of PIAs, etc. Relevant staff should be trained on these policies.
- *Review and update contracts*: Contracts with third party data processors, eg benefit consultants, administrators, actuaries, should be reviewed and updated to include at least the contractual provisions mandated by the GDPR. Also, review liability clauses and indemnities to see if the risk allocation is still appropriate. This is particularly important in view of the fact that data processors now also have statutory obligations and that, in areas like security, both the data controller and the data processor have the same obligation.
- *Watch this space*: The General Scheme of Data Protection Bill 2017 was published by the Department of Justice and Equality in May 2017 and is intended to give effect to, and provide for derogations from, the GDPR. The Bill is currently at a preliminary stage and, therefore, is likely to change a good deal before it is enacted. In addition, we expect the Article 29 Working Party and the DPC to issue various guidance papers clarifying GDPR obligations.



Key Contacts

Peggy Hughes
Partner, Head of Pensions
+353 1 614 2458
phughes@mhc.ie

Peggy leads the Pensions team within our Employment & Benefits team. She is an experienced pensions lawyer who has worked in-house and in private practice on pension law related matters.

Peggy has advised sponsoring employers, both Irish and multinational, trustees of pension schemes (both lay and professional) and individuals on a wide range of pensions-related issues including their respective obligations, duties and rights under the relevant law, service/contractual and pension scheme documentation.

Stephen Gillick
Partner, Pensions
+353 1 614 2198
sgillick@mhc.ie

Stephen is a partner in our Employment & Benefits team, specialising in pensions law. He has extensive experience in advising trustees, sponsoring employers and pension providers on a range of issues, including pension scheme establishment; pension scheme funding and exercises to reduce scheme liabilities.

Stephen regularly presents on pensions related topics and is the current Chair of the Law Society of Ireland Pensions Committee.

Philip Nolan
Partner, Head of Privacy & Data Security
+353 1 614 5078
pnolan@mhc.ie

Philip is a partner and leads our Privacy & Data Security team. Philip's market leading international practice supports some of the world's most successful tech companies. Philip solves complex global privacy problems for major technology multinationals. At present, Philip and his team are heavily involved in GDPR compliance projects for both its multinational and domestic clients.

Dublin London New York San Francisco

MHC.ie