Pensions Authority
Data Protection
Considerations for Trustees of Occupational Pension Schemes

1 INTRODUCTION

The General Data Protection Regulation (**GDPR**) came into force in all EU Member States on 25 May 2018. Compliance is required from 25 May 2018.

Although the GDPR builds on existing data protection concepts, its ultimate aim is to effect a fundamental change in the culture of data protection by those processing personal data. It introduces significant changes that require anyone processing data to invest time and resources into assessing their approach to data protection compliance.

As an EU Regulation which is binding across all Member States, the GDPR harmonises data protection law across the EU to a greater degree than was the case under the previous data protection directives. The GDPR is complemented by the Data Protection Act 2018, (referred to together with previous acts as the Data Protection Acts 1988 to 2018).The Data Protection Act 2018 provides for the permitted national derogations from the GDPR and establishes the administrative and enforcement regime necessary to give effect to the GDPR principles.

This note provides a summary of the key aspects of the GDPR, gives an overview of what the potential impact on trustees might be and an indication of some of the actions that should be considered on an ongoing basis.

Purpose and status of this note

This note is provided for information purposes only, to assist trustees in preparing for the GDPR and to assist in ongoing compliance. While the Authority has made every effort to ensure that the information contained within this note is correct and accurate, nevertheless it is possible that errors and omissions in the content may occur from time to time. It is also worth noting that the legislation and guidance in this area is continuing to evolve and trustees should therefore obtain their own advice from time to time, as necessary.

No liability whatsoever is accepted by the Pensions Authority, its servants or agents for any errors or omissions in the information or data or for any loss or damage occasioned to any person acting or refraining from acting as a result of the information or data contained within this note.

Further information regarding the GDPR and data protection requirements generally is available at www.dataprotection.ie.

Why should trustees care about the GDPR?

Data is at the core of trustees' primary responsibilities. As part of the everyday running of a pension scheme, trustees will be responsible for the collecting and processing of members' personal data. Personal data provided by members is used to determine how to calculate the benefits that should be paid, when they should be paid and to whom they ought to be paid. All of these uses involve personal data being processed.

Although the processing activities themselves are often carried out by third parties such as administrators, trustees remain at all times ultimately responsible for the members' (and other persons') personal data that has been collected by or on behalf of the trustees. As a result, trustees are generally data controllers of personal data which they collect and process and accordingly have certain responsibilities under the GDPR to adhere to in relation to the processing of personal data. Trustees will need to ensure, amongst other things, that all data processing is fair, that personal data is kept secure and that unnecessary or excessive personal data is not collected or processed.

It is important to be aware that "processing" covers a wide range of activities such as collecting or receiving data, sharing data with third parties, storing or archiving data, inputting data onto IT systems or deleting data. Even the mere retention of personal data in manual or electronic files may amount to processing.

The new potential administrative sanctions of up to €20m or 4% of the global annual turnover (if greater) which can be imposed by the supervisory authorities under the GDPR has understandably gained a considerable amount of attention and has increased the risk profile for data protection compliance/non-compliance generally. While it remains to be seen how these fines would be calculated and imposed in a trustee context, it is clear that data protection compliance ought to be a key compliance concern for trustees, given the potential consequences for non-compliance.

The basics

A lot of the data protection rules that trustees should already be familiar with under the current data protection regime are still relevant under the GDPR but have been significantly expanded.

There are a number of **core principles of data protection** that remain at the centre of proper data protection practices as follows:

- personal data must be processed **lawfully, fairly and in a transparent manner** in relation to the data subject;

- personal data must be processed for **specified, explicit and legitimate purposes** and **not further processed** in a manner incompatible with those purposes;
- personal data processed must be **adequate, relevant and limited** to what is necessary in relation to the other purposes for which it is processed;
- personal data must be **accurate**, and where necessary kept **up to date;**
- personal data must be kept **safe and secure;**
- personal data must be retained for **no longer than is necessary**; and
- the GDPR also introduces a **new concept of accountability**, which requires controllers (such as trustees) to be able to demonstrate how they comply with the data protection principles.

The following are some definitions of key data protection terms:

- **Personal Data:** Personal Data is any information relating to a Data Subject.
- **Data Subject:** The identified or identifiable living individual who is the subject of the personal data. An individual is identifiable if they can be identified directly or indirectly, including by name, an identification number (e.g. member number), location data, on-line identifier or otherwise.
- **Special Categories of Data:** Certain categories of data are afforded a higher level of protection than other personal data. These are data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, "genetic data" and "biometric data".
- **Genetic Data:** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that person (personal data resulting, in particular, from an analysis of a biological sample).
- **Biometric Data:** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that person (e.g. facial images).
- **Processing:** Processing means any operation performed upon personal data, whether or not by automated means. These include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Data Controller:** Controller means the natural or legal person, public authority, agency or any other body which alone (or jointly with others) determines the purposes and means of the processing of personal data.

- **Data Processor:** Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

- **Consent:** "The consent of the data subject" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

- **Data Breach:** A Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Health Data:** means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.

- **Profiling:** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict that persons performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- **Pseudonymisation:** means the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without additional information provided that the additional information is kept separately and is subject to technical and organisational measures to ensure that the data cannot be attributed to a specific data subject.

- **Supervisory authority:** is the regulator responsible for monitoring compliance with data protection legislation including the GDPR. In Ireland the supervisory authority is the Data Protection Commission.

2 GOVERNANCE AND AWARENESS

Key points

- The GDPR introduces a number of "data governance" concepts designed to ensure that data protection is taken seriously and to reduce the risk of breaching the GDPR obligations. These include:
    - The concept of data privacy "**by design and by default**". That means that data controllers are expected to take proactive steps to *design* and implement systems and processes which ensure that, as a *default* and from the outset, appropriate standards are maintained when processing personal data.
    - The idea of data privacy by design and default goes hand in hand with the **principle of accountability**. The new principle of accountability requires data controllers to be able to demonstrate how they comply with data protection principles. This requirement to demonstrate compliance runs through the core of the GDPR.
- The GDPR prescribes a number of practical measures to complement these concepts and to ensure sufficient time and resources are allocated to data protection. These include:
    - **Data Privacy Impact Assessments (DPIAs):** the GDPR requires controllers to carry out documented impact assessments for **high risk** processing. The aim is to assess the need for, and the potential benefit of, the processing against the impact on the relevant data subjects.
    - **Data register:** organisations must also keep a record of their processing activities. The record must include a description of the categories of personal data and data subjects, the categories of recipients to whom the personal data is or may be disclosed, the legal grounds relied on for processing, details of transfers of personal data outside of the European Economic Area (**EEA**), the envisaged periods of retention of the different categories of data, and where possible, a general description of the technical and organisational security measures in place. These records must be made available to the supervisory authority, if requested.
    - **Contracts with service providers (data processors):** the GDPR imposes a high duty of care upon controllers in selecting their personal data processing service providers. Contracts must be implemented with such service providers which include a range of specified information and obligations.

- **Data Protection Officers:** some controllers and processors will have to create a new role within their organisation with specific responsibility for data protection called a Data Protection Officer (see page 13).

Impact on trustees

The GDPR aims to establish a new culture of privacy by requiring data privacy to be embedded into a business or organisation. It requires controllers to implement a wide range of measures. It is essential that trustees build data protection compliance into their 'ways of working' so that they are in a position to comply and explain how they comply.

Action points for trustees

- Who will be **responsible** for data protection compliance on behalf the trustees?
- **Consider reporting lines**. Data protection should be a key consideration for the trustees and is not something that can be delegated and forgotten about.
- Data-mapping. It may be helpful for trustees to identify and map their data flows and the processing being applied to personal data in order to assess current data practices and whether they will meet the GDPR compliance criteria. This is often referred to as '**data mapping**'. When carrying out this exercise, it is important to consider and document absolutely every activity carried out on personal data.
- **Record- keeping**. Trustees will then need to consider how they will comply with the requirement to maintain detailed records of data processing activities and how they will satisfy the accountability requirement i.e. demonstrate that their processing activities are in line with the new rules. Record- keeping of processing activities and maintaining a Data Register will likely need to be incorporated as a regular and continuous process of trustees. Trustees should bear in mind they may be required to make the Records available to the supervisory authority on request, so as to demonstrate how compliance with the GDPR is achieved.
- **Compliance plan**. Trustees should put a plan in place to bring data protection practices in line with the GDPR requirements. This might incorporate features such as Data Processing Impact Assessments (**DPIAs**) audits, policy reviews and updated training and awareness raising programs. Trustees need to assess whether they should appoint a Data Protection Officer and should document their decision if they decide not to. Existing supplier arrangements may need to be audited along with any template contracts used by the trustees to reflect the GDPR's data processing obligations.
- **Ongoing and continuous monitoring and awareness of personal data processed**. Compliance with the GDPR is not a "once-off" exercise. It requires a

continuous and ongoing review of personal data processed, the legal basis for processing and the impact of processing on individual's fundamental rights. Trustees should, therefore, ensure that data protection, and their policies and procedures in relation to same, are regular agenda items.

3 LEGAL BASIS FOR PROCESSING

Key points

- As under the current data protection regime, data processing will only be lawful if trustees can point to one of the specified legal bases for processing. The grounds for processing personal data remain largely the same under the GDPR, although consent may become more difficult to rely upon to legitimise processing.
- Data Subjects must be clearly informed of the legal basis relied upon by trustees for the processing of their personal data in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*". This obligation may be satisfied by furnishing a Privacy Notice to data subjects (further information on Privacy Notices is contained in section 4).
- The most relevant grounds for processing personal data by trustees might include the following:
  - **Legal obligation:** the processing is necessary for compliance with a legal obligation to which the data controller is subject e.g. obligations arising under trust law generally and/or under the Pensions Act 1990 (as amended).
  - **Legitimate interests:** personal data may be processed on the basis that the controller has a legitimate interest in processing that data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.
  - **Contractual necessity:** the processing is necessary in order to enter into or perform a contract with the data subject.
  - **Processing of health data for pension purposes**: The Data Protection Act 2018 provides for health data to be processed where necessary and proportionate for pension purposes, provided certain additional suitable and specific safeguards are taken.
  - **Consent:** personal data may be processed on the basis that the data subject has consented to such processing.

Special categories of data

Added difficulties may arise in the case of "special personal data". This is a concern for trustees who process data revealing amongst other things, a member's racial or ethnic origin, physical or mental health, trade union membership or his or her sexual orientation.

Outside of obtaining the explicit consent of the data subject, the grounds under which these categories of data can be lawfully processed are extremely narrow. These include:

- Where the processing is necessary for carrying out obligations of the controller in the field of employment;
- Where the processing is carried out for a not-for-profit organisation;
- Where the information has been made public by the data subject;
- Where the processing is required for the purpose of obtaining legal advice, or of the purposes of exercising or defending legal claims; or
- Where the processing is necessary for medical purposes, including the assessment of the working capacity of the employee.

The trustees would need to consider and determine whether the grounds apply in any particular case.

As mentioned above, the Data Protection Act 2018 provides a derogation that appears to allow pension providers to process 'Health Data' (see definitions) without members' explicit consent. This is subject to "*suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects*" and provided it is necessary and proportionate for "*an occupational pension, a retirement annuity contract or any other pension arrangement*". There are number of other derogations that may be relevant to trustees and/or occupational pension schemes in the Data Protection Act 2018. For example, individuals' rights and controllers' obligations are restricted to the extent necessary and proportionate to protect legal professional privilege (this might be relevant to communications by trustees with their lawyers for the purpose of seeking or receiving legal advice that contain personal data). Trustees should consider all the derogations that may be relevant to their obligations as data controllers, or to the exercise by data subjects of their rights (for example, where a member makes a subject access request).

Consent

There has been a significant change in the approach to 'consent' under the GDPR. To demonstrate a data subject's consent, it must be given by a "*clear affirmative act*" which established a "*freely-given, specific, informed and unambiguous*" indication of agreement. Silence, pre-ticked boxes or inactivity no longer constitute "consent".

Consent will not be regarded as freely given if the data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment. When assessing if consent has been freely given "utmost account" must be taken of whether or not that the performance of a contract or, in the case of trustees, provision of benefits is conditional on consent.

Another complication with relying on consent is that consent can be withdrawn at any time, a right which must be notified to data subjects. If a data subject were to exercise this right, it may make it difficult (if not impossible) for trustees to manage the pension scheme or administer benefits under it. Reliance on consent for processing will, therefore, need to be carefully considered by trustees and in many cases may not be the appropriate legal basis for data processing.

Impact on trustees

Where trustees do currently use the consent justification, they will need to determine if this is still appropriate or whether an alternative legal basis must be relied upon for processing personal data.

The new record-keeping obligations in the GDPR require trustees to retain records of the results of any action taken in relation to processing personal data or to address gaps in non-compliance. This will include recording the legal basis relied upon for processing in addition to the assessment undertaken to justify that legal basis.

Action points for trustees

- For each processing activity identified in the data mapping exercise, trustees should identify the legal basis relied upon for such processing and record it along with recording their justification for relying on that legal basis. This should be reviewed on a regular basis to ensure it is accurate and up to date.

4 COMMUNICATING PRIVACY INFORMATION

Key points

- Under the GDPR, trustees must provide a certain minimum amount of information to members (and any other individuals whose personal data the trustees process e.g. dependants and beneficiaries) in order to comply with the principle of fair and transparent processing. This should happen in particular at the following times in the data processing cycle:
    - When the data is initially collected or obtained;
    - If data is later used for an alternate purpose to that which it was originally collected for;
    - If an individual exercises one of their rights in relation to their data (dealt with in more detail below); and
    - If there is a sufficiently serious breach of the GDPR.
- **Privacy notices** are a key way to communicate with data subjects. Privacy notices must comply with the principle of transparency – they must be easy to understand and should be written in clear and plain language. A change to the processing activities or legal basis relied upon for processing should be recorded in an updated privacy notice.
- A privacy notice must contain at least the following core information:
    - the trustees' names and contact details (as data controllers);
    - the contact details of the Data Protection Officer (if there is one);
    - the purpose of the processing and the legal basis upon which it will be carried out;
    - full details of any third parties with whom the personal data will be shared;
    - details of safeguards that will be employed if data is to be transferred outside the EEA;
    - the period for which the personal data will be stored or the criteria used to determine this period; and
    - details of the individual's rights in relation to the processing, and details of how to exercise those rights.

- If personal data is not obtained directly from the data subject (e.g. member information obtained from the employer or beneficiary information obtained from the member), the data subject must also be informed from whom the information was obtained and the categories of data concerned. This must be provided:
    - no more than one month after the data is obtained; or
    - if the personal data is used for communication with the data subject or is disclosed to a third party, at the time of the first communication with the data subject or the time of disclosure of the data, if earlier.

Impact on trustees

These information requirements will affect all trustees. Trustees will need to devise a communications plan with members to enable them to provide all the information listed above. It is likely that a certain amount of preparatory work will be required to establish this information before it can be translated into privacy notices.

Action points for trustees

- Trustees as data controllers should:
    - Review their privacy notices to assess compliance with the additional information requirements mandated by the GDPR and update privacy notices where required; or
    - Issue new GDPR compliant privacy notices to members and other data subjects.
- It may be unlikely that privacy notices used before GDPR came into effect on 25 May 2018 will satisfy the new GDPR requirements especially considering the GDPR requirement that the privacy notice be transparent. If the privacy notice is not clear and easy to understand even the parts that remain relevant may require revising.

5 SUBJECT ACCESS REQUESTS

Key points

- Individuals already have the right to access their personal data held by trustees by making a "subject access request". The GDPR increases the amount of information to be given by trustees when responding to such requests. Responses will have to include:
    - the period the data is retained for or the criteria used to determine that period;
    - the categories of personal data processed;
    - information on the individual's additional rights under the GDPR and the right to complain to the supervisory authority;
    - details of any automated processing, including profiling and the logic involved, the significance and envisaged consequences of the processing for the data subject; and
    - where data is transferred outside of the EEA, the appropriate safeguards that are put in place.
- The time period for dealing with requests has been reduced from 40 days to 1 month.
- Controllers can no longer charge a fee for responding to a subject access request (unless the requests are for additional copies of the data or are manifestly unfounded or excessive).

Impact on trustees

Trustees should be aware that there may be an increase in access requests from data subjects which may necessitate additional resources.

Action points for trustees

- Procedures for handling subject access requests should be reviewed and updated to provide for the additional information which data subjects are entitled to and which take into account the more limited time period to respond to such requests.
- Consideration might be given to putting in place template response letters to subject access requests.

6 NEW RIGHTS FOR INDIVIDUALS

Key points

Under the GDPR, data subjects' rights are expanded to include:

- **The right to be forgotten:** data subjects are entitled to require a controller to delete their personal data if the continued processing of that data is not justified. The controller does not need to delete the data if an exception applies, including that the processing is needed to comply with a legal obligation.

- **The right to restrict processing:** in some circumstances a data subject may not be entitled to erase their personal data, but may be entitled to limit the purposes for which the controller can process that data.

- **Right of data portability:** Data subjects have the right to transfer their personal data between controllers (e.g. to transfer personal data to another pension provider).

- **Right to object to processing:** data subjects are entitled to object to processing where the controller is processing his or her data on the basis of either "public interest" or " legitimate interests". Unless the controller can demonstrate compelling legitimate grounds, the controller will be required to cease processing.

- **Right to not be evaluated on the basis of automated processing:** data subjects have the right not to be evaluated in any material sense (e.g., in connection with offers of employment; supermarket discounts; insurance premiums; or howsoever) solely on the basis of automated processing of their personal data and can request human intervention in making the decision.

Data subjects also have the right to make a complaint to the relevant supervisory authority in the place where they reside, work or where the alleged infringement of data protection law occurred. Data subjects may also bring proceedings in the courts where they believe their rights under GDPR have been infringed and may be able to claim damages.

Impact on trustees

These new rights provide members and other data subjects with increased control over how trustees process their personal data, for example, by allowing them to object to processing where it is based on the legitimate interests of the trustees. Trustees will need to have processes and procedures in place to deal with requests from members seeking to exercise these new rights.

Action points for trustees

- All relevant people should be informed of these new rights and procedures should be implemented to ensure the rights are respected.

- Data Privacy Notices and policies may need to be reviewed, revised or put in place to ensure these new rights are catered for.

- Appropriate systems will be required to deal with the right to erasure, restriction of processing and data portability (as applicable).

7 DATA BREACHES AND ACTIONS TO BE TAKEN

Key points

- A significant new requirement under the GDPR is the uniform breach notification rule across the EU, which requires EU data controllers to notify their supervisory authority of a Data Breach (see definitions section) within 72 hours, unless the breach is unlikely to result in a risk to the rights of data subjects.
- Controllers will also have to notify data subjects where the breach is likely to result in a "high risk" to affected data subjects. This requirement may not apply if the controller has subsequently taken steps to ensure that the high risk to the individual is no longer likely (for example if the controller has taken steps to render the personal data unintelligible to anyone not authorised to access it, such as encryption). A public communication may be issued to inform data subjects if giving individual notification would involve disproportionate effort.
- Where a breach affects data subjects in more than one Member State, and notification is required, the controller should report the breach to its lead authority (very generally, the supervisory authority in the country where the controller has its "main establishment" within the meaning of the GDPR).
- A controller may wish to proactively report the incident to a supervisory authority which is not its lead authority, if it is aware that individuals in other Member States are affected by the breach.
- Processors are only obliged to report data breaches to controllers.

Impact on trustees

The current law contains no legal obligations to notify the relevant supervisory authority or affected data subjects of personal data breaches (although the Data Protection Commission has issued a non-binding code of practice). It will now be mandatory to report data breaches in all circumstances where there is a risk to the rights of data subjects.

Even the best run organisations can suffer security breaches from time to time and trustees must be prepared to take action, should a breach occur. Trustees must also be aware that they, as data controllers, will be responsible for notifying breaches caused by the scheme administrator, or other third parties who process data on behalf of the trustees.

Action points for trustees

- Trustees should carry out a review of their security measures and consider if they are robust enough to meet the requirements of the GDPR. If possible, data should be unintelligible in the case of unauthorised access.

- Trustees should consider adopting a data breach policy, including identifying individuals or teams who will take the lead in responding to a breach.
- Data processing agreements with scheme administrators and other third parties should be reviewed to ensure they include a requirement for the processor to immediately inform the trustees of any data breaches, and assist them in complying with their notification obligations.
- The supervisory authority has indicated that breach notifications will be monitored carefully and controllers who notify insignificant or potential breaches may run the risk of being sanctioned.

8 DATA PROTECTION OFFICER REQUIREMENTS

Key points

- The GDPR creates a new obligation on certain controllers and processers to appoint a Data Protection Officer (DPO). A DPO must be appointed if the controller or processor:
    - is a public body;
    - if their core activities require regular and systematic monitoring of data subjects on a large scale; or
    - if their core activities involve large scale processing of sensitive data and data relating to criminal convictions.
- The DPO will be responsible for:
    - Raising GDPR awareness including training relevant individuals and advising on the organisation's data protection policies;
    - record-keeping (e.g. creating inventories and keeping a register of processing operations); and
    - monitoring GDPR compliance, acting as the supervisory authority's main point of contact and assisting with addressing, or taking steps in relation to, any actual or potential breaches that may occur.
- However, responsibility for compliance with the GDPR continues to rest with the controller or processor, not with the DPO.
- One DPO can be appointed for a group of undertakings provided he or she is "easily accessible" from each establishment.
- DPOs appointed voluntarily (where the controller/processor does not think their appointment is strictly required) are likely to be subject to the same obligations and responsibilities as obligatory DPOs.

Impact on trustees

Pension schemes process a large amount of data, which can include sensitive or Special Categories of Data. It is not clear whether this would count as a "core activity", particularly where the processing of data is outsourced by controllers.

Another consideration is whether trustees' activities would be considered 'large scale'. The GDPR does not define the terms, but guidance issued by the Article 29 working party

recommends that the following factors are considered in assessing whether large scale processing is being carried out: (a) the number of data subjects; (b) the volume of data; (c) the duration of processing; and (d) the geographical extent of the processing.

Action points for trustees

- Consider whether the DPO requirements apply, taking advice if necessary.
- Document the analysis if it is decided not to appoint a DPO. If trustees appoint a person to be responsible for data protection where they do not think it is strictly necessary (e.g. a more general privacy officer), trustees should consider documenting the rationale for not appointing an official DPO, which may assist in preventing that person being subject to the same statutory obligations.

9 INTERNATIONAL DATA FLOWS AND REQUIREMENTS.

Key points

- The rules around data transfers to countries outside the EEA are not significantly changed by the GDPR. The GDPR prohibits the transfer of data to countries outside the EEA, unless that country ensures an 'adequate level of protection', as specified by the European Commission.
- The GDPR, like the current data protection regime, permits transfers to third countries where "appropriate safeguards" are put in place between the transferor and transferee, such as binding corporate rules (a set of rules put in place between group companies to ensure that adequate data protection practises are employed worldwide) or model clauses (a set of standard contractual clauses approved by the Commission that can be entered into between transferor and transferee to ensure data transferred will be adequately protected).
- The GDPR includes two additional mechanisms – reliance on an approved code of conduct or on an approved certification mechanism.
- The GDPR permits transfers to third countries in specified situations, including where:
    - the data subject has explicitly consented to the transfer;
    - the transfer is necessary for the performance of a contract;
    - for public interest reasons;
    - the defence of legal claims; or
    - the vital interests of the data subject.
- Where none of the other safeguards or derogations apply, the GDPR permits a transfer to a third country if it is necessary for the compelling legitimate interest of the controller, it is not repetitive, it concerns only a limited number of data subjects and the controller has provided suitable safeguards. The controller must inform the supervisory authority of the transfer.
- The GDPR prohibits any non-EEA court, tribunal or regulator from ordering the disclosure of personal data unless it requests such disclosure under an international agreement, such as a mutual legal assistance treaty.

Impact on trustees and action points

- The rules around data transfers outside the EEA will not change significantly under the GDPR. However, in the course of reassessing current data protection practices

and putting plans in place, it would be prudent for trustees to also review their data flows and ensure they have the appropriate international data transfer mechanisms in place.