# GDPR: IMPLICATIONS FOR TRUSTEES AND PERSONAL REPRESENTATIVES



A guide to the General Data Protection Regulation ((*EU) 2016/679*) (GDPR) for trustees of private trusts and personal representatives of deceased estates.

by *Practical Law Private Client* and *Suzanne Rab, Serle Court*

RESOURCE INFORMATION

RESOURCE ID
w-013-7137

RESOURCE TYPE
Practice note

PUBLISHED DATE
11 April 2018

JURISDICTION
United Kingdom

## CONTENTS



## SCOPE OF THIS NOTE

The General Data Protection Regulation ((*EU) 2016/679*) (GDPR) will introduce a new EU data protection regime in the UK from 25 May 2018. Although trustees and personal representatives (PRs) have previously been subject to data protection rules, the introduction of the GDPR regime represents a tightening up of the obligations owed by them and an extension of some of the obligations to agents such as solicitors and other professionals and suppliers working for them.

The GDPR is designed to ensure that personal data is processed in such a way that the rights of individuals (data subjects) are protected. In the context of trusts and estates, trustees and PRs will owe duties to beneficiaries as data subjects.

The implementation of new data protection rules in the UK is subject to three phases in 2018:

- Until 25 May 2018, the applicable regime for data protection in the UK is contained principally in the Data Protection Act 1998 (DPA 1998).
- From 25 May 2018, the GDPR will be directly applicable in the UK and in all other EU member states.
- The UK Data Protection Act 2018 (DPA 2018) makes changes to UK law on data protection, repealing the DPA 1998 and making provision for the exercise by the UK of various derogations permitted by the GDPR and other related amendments. The DPA 2018 enters into force on 25 May 2018. It applies to both cross-border and domestic processing of personal data. The DPA 2018 provisions will align UK law with the GDPR, so that on Brexit, although the GDPR will no longer have direct legal effect in the UK, UK data protection law is expected to remain aligned to EU data protection law. To track progress of the DPA 2018, see *Data Protection Bill 2017-19: tracker.*

Complying with the GDPR (or equivalent provisions) is expected to be mandatory in the UK, regardless of the outcome of the UK's negotiations on the terms of withdrawal and so that transfers of data to and from the UK will not require any specific authorisation (*Article 45, GDPR*). Therefore, despite Brexit, trustees and PRs should continue to plan for the introduction of the GDPR. For more information on the implications of the UK having third-country status following withdrawal from the EU, see *Practice note, Overview of EU General Data Protection Regulation: UK perspective.*

Professionals acting for trustees and PRs will either be data processors (broadly, any entity or individual that processes personal data on a data controller's behalf) or joint data controllers with the trustees or PRs. Data processors such as solicitors and accountants working for trustees and PRs will be subject to new data protection obligations under the GDPR. Although this note focuses principally on the obligations of data controllers, it also touches on the obligations that apply directly to data processors acting for them. For more materials that can help professional adviser organisations to comply with their GDPR obligations as data processors, see *EU General Data Protection Regulation toolkit.*

This note does not consider the implications of the GDPR for trustees of charitable trusts, pension trusts or employee benefit trusts. For more information on the GDPR and charities, see *Legal update, GDPR: new overview guidance for charities and fundraisers*. For information on the GDPR implications for pension trustees, see *Practice note, Pensions and data protection: preparing for the General Data Protection Regulation.*

For a general introduction to the GDPR, see *Practice note, Overview of EU General Data Protection Regulation.*

## TRUSTEES AND PRS AS DATA CONTROLLERS

Most obligations under the GDPR fall on the data controller: the person who, alone or jointly with others, determines the purposes and means of the processing of personal data (*Article 4(7), GDPR*). The GDPR defines personal data as any information relating to an identified or identifiable natural person (the data subject). It applies to any processing, including collecting, recording, organising, storing, retrieving, consulting, using, erasing or destroying the personal data (*Article 4(2), GDPR*). Trustees and PRs are clearly data controllers in relation to the information they gather, store and use about trust and estate beneficiaries who are natural persons (but not in relation to beneficiaries that are non-natural persons such as charities or other non-natural organisations) (see *Example 1: are trustees or PRs data controllers?*).

On a strict interpretation, the GDPR does not apply to the personal data of deceased persons (*recital 27, GDPR*). The information about a deceased settlor or testator held by trustees and PRs will not be subject to GDPR obligations, although the common law duty of confidentiality owed to a settlor or testator continues after they have died.

Although trustees and PRs often volunteer their services to the settlor or testator on a non-professional unpaid basis, the GDPR duties will still apply to them as they apply to professional, paid trustees and PRs. There is an exception for data processed in a purely personal or household context (*Article 2(2)(c), GDPR*), but this is unlikely to extend to trustees holding beneficiary data as they will be acting in a fiduciary capacity. Data processing is only covered by the household exception where the processing is carried out in the course of the private or family life of individuals. To come within this exception, the processing must have no connection to a professional or commercial activity (*recital 18, GDPR*).

However, the obligation to maintain a record of processing activities under Article 30 of the GDPR does not apply to enterprises or organisations employing fewer than 250 people, unless any of the following apply:

- The processing it carries out is likely to result in a risk to the rights and freedoms of data subjects.

- The processing is not occasional.
- The processing includes special categories of data as referred to in Article 9(1) of the GDPR.
- The processing includes personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR.

This exception may apply to many trustees and PRs and some professional advisers providing services to them (see *Exceptions*).

## GDPR PRINCIPLES

The GDPR sets out several principles which data controllers and processors must comply with when processing personal data (*Article 5, GDPR*). These principles form the core of the obligations of the data controller and will usually form the basis of any claim that a data controller has not complied with their statutory duties.

Article 5 of the GDPR includes the following principles:

- Lawfulness, fairness and transparency. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (*Article 5(1)(a), GDPR*).
- Purpose limitation. Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. (*Article 5(1)(b), GDPR*.) As a general rule, the purpose limitation principle binds the data controller to the specified, explicit and legitimate purposes notified to the data subject on collection of the personal data (*Article 5(1)(b), GDPR*). Further processing of the data beyond that which was originally anticipated is only permitted as long as the new processing activity is not incompatible with that original purpose. Further processing of personal data for a purpose that is incompatible with the original purpose is only permitted if the data subject consents to this new processing activity (*Article 6(4), GDPR*). This presents particular problems for trustees and PRs because the personal data they control and the purpose behind the processing will often be dictated by a third party; the settlor or testator. Beneficiaries may be unaware that their personal data is being controlled by the trustee or PR and they may not fully understand the purpose behind the processing.
- Data minimisation. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (*Article 5(1)(c), GDPR*).
- Accuracy. Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (*Article 5(1)(d), GDPR*). For further discussion, see *Keeping data subject information up to date.*
- Storage limitation. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (*Article 5(1)(e), GDPR*). For further discussion, see *Policy on storage limitation.*
- Integrity and confidentiality. Personal data must be processed in a manner that ensures its appropriate security (*Article 5(1)(f), GDPR*). This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Data controllers and processors must therefore use appropriate technical or organisational security measures. For further discussion, see *Keeping personal data of data subjects safe.*
- Accountability. The data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles (*Article 5(2), GDPR*).

Compliance may necessitate trustees and PRs developing a record-keeping protocol or checklist (see, for example, *Practice note, Trustee record-keeping requirements* (this is in the context of pension trustees but may be useful as a starting point)).

### Transparency principle

In addition, data subjects have a right to receive information about:

- The identity of the data controller and the nature of the processing (*Articles 13 and 14, GDPR*) (see *Privacy notices*).
- Whether or not their personal data is being processed and, if so, the nature of and purpose behind processing (*Article 15, GDPR*).

- Any personal data breach when that breach is likely to result in a high risk to their rights and freedoms (*Article 34(1), GDPR*).

## LAWFUL GROUNDS FOR PROCESSING DATA

A data controller must only process personal data on the basis of one or more of the following legal grounds (applied separately to each purpose) set out in Article 6 of the GDPR:

- Consent. The data subject has given their consent to the processing of their data for one or more specific purposes (*Article 6(1)(a), GDPR*).
- Contractual obligation. It is necessary for entering or performing a contract with the data subject (*Article 6(1)(b), GDPR*).
- Legal obligation. It is necessary for compliance with a legal obligation to which the data controller is subject (*Article 6(1)(c), GDPR*).
- Vital interests of data subject. It is necessary to protect the vital interests of the data subject (*Article 6(1)(d), GDPR*). Recital 46 to the GDPR makes it clear that this ground will generally only apply to matters of life and death or other humanitarian grounds and should only be used if the processing cannot be based on one of the other grounds.
- Public interest. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed (*Article 6(1)(e), GDPR*).
- Legitimate interests. It is necessary for the purposes of legitimate interests pursued by the data controller or by a third party, except where these interests are overridden by the interests or the fundamental rights and freedoms of the data subject (*Article 6(1)(f), GDPR*). When determining whether the data subject's interests or fundamental rights and freedoms override the data controller's legitimate interest, the data subject's reasonable expectations based on the relationship with the controller must be taken into account (*recital 47, GDPR*). The interests and fundamental rights of the data subject could, in particular, override the interest of the data controller where personal data is processed in circumstances where data subjects do not reasonably expect further processing.

### Which legal grounds can trustees and PRs use?

In most cases, personal data about beneficiaries will be supplied by the settlor or testator or gathered without beneficiary consent. Consent is therefore unlikely to be a ground that could be used by trustees and PRs. Also, if consent to processing is relied on, additional obligations will apply to the data controller and beneficiaries will have additional rights including a right to withdraw the consent so that data can no longer be processed, data portability rights and the right to have the personal data erased.

The most relevant legal ground for processing personal data is likely to be that trustees and PRs are legally obliged to hold information about the beneficiaries (and, conceivably, other family members or individuals who had a relationship with the settlor or testator) as part of their duties in running the trust or administering the estate.

Processing for the purposes of a data controller's legitimate interests could also be pleaded. However, guidance on this ground published by the Information Commissioner's Office (ICO) notes that it may result in more work for the controller or processor as there is likely to be more scope for disagreement when balancing the interests of the controller against the rights of beneficiaries. For more information, see *ICO: Legitimate interests.*

## SPECIAL CATEGORY DATA

Processing data about a beneficiary's race, ethnic origin, politics, religion, trade union membership, genetic and biometric data, health, sex life or sexual orientation is prohibited under the GDPR unless certain conditions apply. Among the conditions that might apply in the context of a trust or estate are:

- The beneficiary has given consent.
- The processing is necessary to carry out the obligations and exercise specific rights of the controller or of the beneficiary in the field of employment and social security and social protection law (unlikely to be relevant in the trust or estate context).
- The processing is necessary to protect the vital interests of the beneficiary or of another person where the beneficiary is physically or legally incapable of giving consent.

- The data is manifestly made public by the beneficiary.
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest, so long as this is proportionate to the aim pursued, respects the essence of the right to data protection and there are safeguards in place to protect the beneficiary's rights and interests.

(A*rticle 9(2), GDPR*.)

Trustees and PRs may have access to this type of sensitive data from letters of wishes, trust and testamentary documents. They may also obtain special category data about beneficiaries, other family members and individuals with whom the settlor or testator had a relationship, when considering how the trust fund or estate should be distributed. This prohibition could present an obstacle where considering this type of sensitive information could be essential to exercising powers correctly. Trustees and PRs may be able to argue that it is in the public interest to see that the wishes of a settlor or testator are followed as closely as possible, or that the processing is necessary to establish beneficiary rights (see *Example 3: processing special category data*). This is also a difficult issue for pension trustees and the professional bodies representing them have asked the ICO to provide guidance (as yet not published) on the collection of special category data where it is felt to be essential to support trustees' decision-making. The guidance for pension trustees may also assist trustees of private trusts and PRs. A further issue is that trustees or PRs may not even know that they hold the special category data until the letter of wishes is opened. This raises a question of what they should do in response to a data breach or subject access request before they have seen the letter of wishes. The ICO may produce guidance on this and other unexplored issues in the future especially as it is an area that pension trustees have to grapple with, not just trustees of private trusts.

## BENEFICIARIES' RIGHTS TO INFORMATION

A fundamental principle of trust law is that beneficiaries should have sufficient information about the trust to enforce it and see that the trustees are administering it correctly. For estate beneficiaries, disclosure rules for documents or other information (otherwise than in litigation) are similar to those for trusts. Although there is no automatic entitlement to disclosure (*Schmidt v Rosewood Trust Ltd [2003] UKPC 26*), trustees and PRs have a discretion to disclose and the court will supervise that discretion if it is not exercised properly.

An adult beneficiary who has an interest in possession under a trust is entitled to know of the existence of the trust, and of the nature of his interest under it (*Brittlebank v Goodwin (1868) LR 5 Eq 545*). The position of discretionary beneficiaries is less clear but best practice suggests that trustees should take reasonable steps to inform beneficiaries of the existence and nature of the interest (*Chaine-Nickson v Bank of Ireland (1976) IR 393*), unless they are unlikely to benefit from the trust (*Re Manisty's Settlement Trusts [1974] Ch 17*).

For more information on trust and estate beneficiaries' rights to information, see *Practice notes, Beneficiaries' rights to information* and *Rights of a beneficiary and duties of a personal representative.*

Data protection laws provide beneficiaries with rights to information that can cut across trustees' rights not to disclose at their discretion. Pre-DPA 2018 case law provides some insight on the interaction between data protection law and trustees' rights and duties. *Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74* considered what rights trust beneficiaries have under the DPA 1998 to information about the trust (see *Legal update, Court of Appeal overturns High Court decision and orders subject access compliance*). The court allowed the beneficiaries' subject access request because the DPA 1998 does not contain an exception for documents not disclosable to a beneficiary of a trust under trust law principles. The court also found that the DPA 1998 does not limit the purpose for which a data subject may request their data. This means that trustees and PRs cannot refuse to supply beneficiaries with details of the personal information they hold about them simply because they believe that the beneficiary has a collateral purpose such as mounting hostile litigation. The same principles are likely to apply under the GDPR (see *Example 4: data subject access requests*).

The GDPR makes a distinction between data provided by the data subject and data provided by someone else (such as a settlor or testator). Where data has been provided by someone other than the beneficiary, trustees and PRs may be able to rely on confidentiality obligations owed to the settlor, testator or other beneficiaries to limit what they disclose (*Article 14(5)(b) and (d), GDPR*). However, the court's approach to this limitation under the GDPR is uncertain (*Dawson-Darmer v Taylor Wessing LLP*).

Notably, the Data Protection Bill 2017-2019 includes an exemption from the GDPR obligation to provide data subjects with information about personal data that is processed (see *Privacy notices*) where a claim for legal professional privilege could be maintained in legal proceedings (*paragraph 17, Schedule 2, Data Protection Bill 2017-2019*).

## RIGHTS OF BENEFICIARIES AS DATA SUBJECTS

For a quick guide summary of beneficiary rights, see the table in Key rights of beneficiaries as data subjects.

### Data subject access

Trust and estate beneficiaries, as data subjects, have the right to ask the trustee or PR whether or not they process personal data relating to them (*Article 15, GDPR*).

If the beneficiary's personal data is being processed, the trustee or PR must provide the beneficiary with the following information:

- The purposes behind the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular, recipients in third countries or international organisations.
- Where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period.
- The right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to that processing.
- The right to lodge a complaint with the ICO.
- Where the personal data is not collected from the beneficiary (for example, where it has been provided by the settlor or testator), any available information as to its source.

The trustee or PR must also provide the beneficiary with a copy of the personal data undergoing processing (*Article 15(3), GDPR*), although this should not adversely affect the rights and freedoms of others. Therefore, if this obligation is fulfilled by providing a copy of trust or testamentary documents, trustees and PRs should consider whether each copy should be redacted, limiting the information to that which is directly relevant to the particular beneficiary. The first copy of the information must be provided free of charge but if the beneficiary asks for further copies, a reasonable fee can be charged based on administrative costs.

If the beneficiary makes the subject access request by electronic means (such as by email), trustees and PRs must provide the information in a commonly used electronic form unless otherwise requested by the beneficiary.

Privacy notices

To fulfil their obligation to give access to the information they hold, trustees and PRs should provide beneficiaries with a privacy notice as soon as possible. The GDPR stipulates that the information must be provided within a reasonable period after obtaining the personal data but, at the latest, within one month having regard to the specific circumstances in which the data is processed (*Article 14(3)(a), GDPR*). If the personal data is to be used for communication with the beneficiary (which will be the most likely reason for trustees and PRs holding the data), the information should be provided at the time of the first communication (*Article 14(3)(b), GDPR*). The best method of fulfilling this obligation, therefore, would be to send the privacy notice as part of the first communication with beneficiaries.

Article 14(5) of the GDPR applies a proportionality filter to privacy notices so that it is not necessary to provide one if providing the prescribed information would:

- Be impossible.
- Involve disproportionate effort.
- Seriously impair the achievement of the objectives behind the processing.
- Breach confidentiality obligations (including professional or statutory secrecy obligations).

As the scope of these exceptions is uncertain, in the absence of guidance from the ICO, trustees and PRs should consider providing a privacy notice unless there are compelling reasons not to.

Trustees and PRs must include the following information in a privacy notice to each beneficiary for whom they hold personal data:

- The identity and contact details for the trustees or PRs. Rather than giving details of the whole body of trustees or PRs, they can give details of a representative trustee or PR as a point of contact.
- Where the personal data is provided by a third party (such as the settlor or testator), any available information about the source. The privacy notice could explain that the personal data is set out in the trust deed, will or

letter of wishes or that they were gathered from attendance notes or questionnaires completed when the settlor or trustee gave instructions for the trust or will to be drafted. This will present particular problems if a secret trust or semi-secret trust exists. In these cases, it may be possible to argue that the data protection obligations under the GDPR are trumped by the duty of confidentiality owed to the testator or that disclosing the source of the information would seriously impair the objectives of the processing (*Article 14(5)(b), GDPR*). However, it is not clear whether a court would agree that a duty of confidentiality would be paramount (*Dawson-Darmer v Taylor Wessing LLP*).

- The contact details of any data protection officer (DPO) (this is probably unlikely to be relevant to most modest trusts and estates (although see *Flowchart, Do we need a data protection officer?*)).
- The purpose(s) behind the processing. It is important to set down a comprehensive list of purposes to avoid having to send a follow-up privacy notice. Setting out full details will require careful consideration. Trustees should think about possible reasons why they may require the personal data. Examples that might apply are:
  - corresponding with beneficiaries about distributions and trust or estate accounts;
  - checking that names and addresses are up to date;
  - seeking beneficiary consents (for example, before exercising a statutory power of appropriation);
  - completing certificates of tax deducted or other tax forms;
  - registering an estate or trust with HMRC's Trust Registration Service (TRS);
  - tracking compliance with undertakings in relation to conditional exemption from inheritance tax;
  - collecting information for Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) compliance;
  - bankruptcy searches;
  - asking beneficiaries to verify their identity;
  - enquiring about missing beneficiaries, including the employment of search agents;
  - monitoring certain beneficiaries in relation to rights of occupation;
  - assessing life expectancy of life interest beneficiaries for actuarial or tax indemnity purposes; and
  - assessing the particular financial or physical needs of beneficiaries when deciding whether funds should be distributed to them.
- The legal basis for processing that the trustees or PRs are relying on. In most cases this will be that the processing is necessary to enable the trustees or PRs to comply with a legal obligation (see *Which legal grounds can trustees and PRs use?*).
- The categories of personal data.
- Details of any recipients of the personal data (for example, this could include any data processors such as solicitors and accountants, HMRC, the Probate Registry, Land Registry, bankruptcy search companies, money laundering verification companies, genealogists, and insurance companies).
- If the trustees or PRs intend to transfer personal data to a recipient in a third country or international organisation, information about the adequacy of the data protection regime that applies in that third country. In a trust and estate context, this is most likely to be relevant where a trustee or PR outsources some support or professional services functions. An example might be where a copy of a will which includes the names and addresses of beneficiaries is to be sent to a probate registry in a third country to obtain probate in relation to assets held there.
- The period for which the data will be stored or, if it is not possible to set out a particular period, the criteria used to determine that period. Trustees and PRs may need to retain data for relatively long periods. Therefore, they may prefer to explain the criteria they use to determine how long data should be retained rather than restricting themselves to a precise period. The criteria may be that trustees and PRs must retain the data for as long as necessary to fulfil the legal obligations owed to the beneficiary (for example, for the duration of the trust period, for the duration of the administration of the estate or will trust, or for the limitation period for the bringing of legal claims for breach of trust).
- If trustees and PRs use their legitimate interests as the legal ground for processing the data, they must explain what the legitimate interests are.

- What rights the beneficiary has under the GDPR (for example, right to request access to data, rectification, erasure, restriction or data portability, right to lodge a complaint with the ICO) (see *Key rights of beneficiaries as data subjects*).

Practical Law Private Client plans to produce a standard document privacy notice for use by trustees and PRs. In the interim, Standard document, GDPR Candidate privacy notice (UK) (which is in a relatively short form) could be used as a starting point.

### Right to rectification

Based on the accuracy principle in Article 5(d) of the GDPR (see *GDPR principles*), beneficiaries have the right to request the data controller to:

- Rectify any personal data relating to them that is inaccurate.
- Complete any incomplete data, including by way of supplementing a corrective statement.

This requirement is unlikely to present any additional impacts on trustees and PRs as they will want to ensure that the data they hold is as complete and reliable as possible. However, they should anticipate the data protection context in which a request for rectification might be made.

### Right to erasure ("right to be forgotten")

Beneficiaries and other data subjects have the right to demand that trustees and PRs erase personal data concerning them without undue delay. However, trustees and PRs only need to comply with this type of request if one of the following grounds applies:

- The data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
- The beneficiary withdraws consent where this was the basis for the processing and there is no other legal ground for processing the data.
- The beneficiary objects to the processing of their personal data and the legal ground used for the processing is that it is in the public interest or in the trustee's or PR's legitimate interests. Beneficiary objections can be overcome if the trustee or PR can show that there are compelling legitimate grounds which override the interests, rights and freedoms of the beneficiary.
- The personal data has been unlawfully processed by the trustee or PR.

This right may be invoked where the personal data includes special category data (see *Special category data*) or details of family relationships that are used to decide whether to pay make payments at their discretion. Trustees should therefore be prepared to erase that data where an exception does not apply.

(*Article 17(1), GDPR.*)

Trustees and PRs must erase personal data of beneficiaries if they have made the data public (for example, if they have published the information on the internet) (*Article 17(2), GDPR*). This is unlikely to happen deliberately as trustees and PRs will wish to ensure that all data about beneficiaries is kept secure. In any case, making beneficiary data public may represent a personal data breach which would be subject to sanctions. A will is a public searchable document once a grant of probate has been issued. Arguably, obtaining a grant could be seen as making personal data about beneficiaries public if the will contains the names and addresses of beneficiaries. This is in contrast to beneficiary names and addresses published in a general directory with no connection to the will itself.

### Restriction of processing

Beneficiaries have the right to demand that trustees or PRs restrict the processing of their data in certain circumstances (*Article 18, GDPR*).

The right to restrict processing exists where one of the following conditions applies:

- The beneficiary contests the accuracy of the data. The beneficiary can ask for the data to be restricted for a limited period to give the trustee or PR time to verify that the information is accurate.
- The processing is unlawful but the beneficiary does not want the data to be erased. This could be the case where the beneficiary needs the data for evidential purposes.
- The trustee or PR no longer needs the data to carry out their duties but the beneficiary requires them to retain it for the establishment, exercise or defence of legal claims.

- Where the trustee or PR argues that the data is processed on the grounds of their legitimate interests, and the beneficiary has objected to processing until it can be shown that the trustees or PRs legitimate interests override their own interests, rights and freedoms.

When the right to restrict processing applies, the trustee or PR can still store the data, but may only process it in one of the following circumstances:

- With beneficiary consent.
- For the establishment, exercise or defence of legal claims.
- For the protection of the rights of another natural or legal person.
- For important public interest reasons.

The right to restriction of processing therefore provides a lower level of protection that takes into account the potential usefulness of the data to beneficiaries themselves, or to the trustees or PRs.

(*Article 18(1), GDPR*.)

### Obligation to notify others

Trustees and PRs must also communicate any rectification, erasure or restriction of processing to each recipient to whom they have disclosed the personal data, unless this proves impossible or involves disproportionate effort (*Article 19, GDPR*). They must inform beneficiaries about the recipients to whom they have made the data available (see *Privacy notices*).

### Right to data portability

Article 20(1) of the GDPR introduces a new right to data portability. This means that beneficiaries who have provided personal data to trustees or PRs have the right to obtain, on request, a copy of that data, provided both of the following conditions are met:

- The processing is based on the beneficiary's consent or on a contract.
- The processing is carried out by automated means.

Where this applies, the trustee or PR must provide the data in a structured, electronic format that is commonly used and permits further use by the beneficiary. The right to data portability is unlikely to be relevant in the context of most trusts and estates as it is aimed mainly at online service providers and is designed to promote consumer rights to move seamlessly from one service provider to another.

### Keeping data subject information up to date

The obligation to maintain accuracy may be difficult for trustees and PRs to comply with. It is likely that relevant information about beneficiaries (such as addresses) will change over time, particularly where the information originates from a deceased settlor or testator and is taken from a trust deed or will that was executed many years ago.

However, keeping up-to-date information about beneficiaries has always been best practice for trustees and PRs to enable them to comply with their fiduciary duties. For non-discretionary trusts, the trust may fail if the words used in the trust deed do not enable the trustees to draw up a complete list of all those intended to take an interest under the trust (*Whishaw v Stephens [1970] AC 508*). Trustees and PRs need to keep records of up-to-date names and addresses for all identified beneficiaries to ensure they distribute assets to the right people. Missing beneficiaries should be traced if reasonably possible and beneficiaries' names and addresses should be accurate to ensure that PRs are not held personally liable for distributing the estate to the wrong people.

One possible method for maintaining accuracy is to ask the settlor or testator to inform trustees or PRs of any changes in named beneficiaries' personal data. However, this will only work while the settlor or testator is alive. Alternatively, when sending a privacy notice to beneficiaries (see *Privacy notices*), ask beneficiaries to inform the trustees or PRs of any changes to their personal data. If trustees (including will trustees) must register with HMRC's TRS, up-to-date personal data about beneficiaries must be submitted annually. Compliance with this money laundering obligation could, therefore, be dovetailed with the GDPR accuracy obligation. For more information about trustees' and PRs' obligations to register trust and beneficiary details with the TRS, see *Practice note, Trusts register* and *information obligations for trustees: resources*.

For trusts and will trusts with a wide discretionary class, it may not be necessary for trustees and PRs to process personal data for all those within the class. For example, if the trust or will trust is accompanied by a letter of wishes which makes it clear that some members of the discretionary class are very unlikely to benefit because

they are default beneficiaries, the trustees or PRs may decide that it is not cost-effective to track down names and addresses for this category of beneficiary (see *Example 2: assessing what personal data is held and when to limit it*).

### Policy on storage limitation

Trustees and PRs should produce or review a written policy on storage limitation to demonstrate compliance with the overarching GDPR principle that the data should only be collected for specified, explicit and legitimate purposes. The policy should indicate what steps will be taken to prevent further processing beyond the specified purposes and to ensure that processing is limited to what is necessary. This could involve putting in place a file and record retention policy that sets out a long-stop date beyond which personal data will be securely destroyed or erased. Although drafted for employers, Standard document, Employment records: retention and erasure guidelines could act as a starting point for this type of policy.

### Keeping personal data of data subjects safe

Trustees and PRs should formulate a policy to keep beneficiaries' personal data secure. Lay trustees and PRs may routinely transmit information about beneficiaries using personal email servers. This is unlikely to provide the sufficient level of security to prevent data breaches or cyber hacking. For more information about methods of keeping data safe through encryption (including email encryption and encrypted data storage), see *ICO: Encryption*. If beneficiary data is stored in the cloud by trustees, PRs or their professional advisers, security risks should be considered carefully. For more information, see *Practice note, Data protection aspects of cloud computing (DPA 1998 version)*.

## OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS

For a quick guide summary of the obligations owed by data controllers and processors, in table form, see *Key obligations of data controllers and data processors*.

Trustees and PRs must demonstrate compliance with the data protection regime as part of the overall principle of accountability. Even if some of the obligations are not directly relevant to the particular circumstances of some trustees and PRs or their professional advisers, familiarity with the GDPR obligations as a whole is essential when dealing with requests for information from beneficiaries or accusations from beneficiaries that obligations have not been complied with.

### Appointment of a data processor

Where trustees or PRs delegate data processing functions to data processors (for example, solicitors or accountants), they must enter into a contract with them that imposes the following obligations on the processor:

- Process the personal data only on the documented instructions of the controller, including with regard to international data transfers to any third country or an international organisation. This is likely to mean that data processors cannot use cloud computing technology or services without the data controller's approval.
- Comply with security obligations equivalent to those imposed on the controller (see *Practice note, Data security under the GDPR*).
- Only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality.
- Enlist a sub-processor only with the prior permission of the controller. Where a sub-processor is appointed, the contract between the processor and the sub-processor must reflect the data protection obligations set out in the contract between the controller and the processor.
- Assist the controller in dealing with requests from beneficiaries for information or where beneficiaries seek to exercise their rights as data subjects (see *Rights of beneficiaries as data subjects*).
- Assist the data controller in carrying out its data security obligations (see *Practice note, Data security under the GDPR*).

(*Article 28(3), GDPR*.)

If trustees or PRs request it, the data processor must also delete or return all personal data at the end of the service provision (*Article 28(3)(g), GDPR*).

Data processors must provide information to trustees and PRs that demonstrates that it is complying with its GDPR obligations. This would include enabling and assisting trustees and PRs to carry out data audits and inspections (*Article 28(3)(h), GDPR*).

### Document requirements

Article 30 of the GDPR introduces document requirements for both data controllers and data processors. However, there is an important carve out (subject to some exceptions) for controllers or processors employing fewer than 250 people, which may exclude some trustees or PRs and some processors (see *Exceptions*).

#### Obligations of the data controller

Trustees, PRs not subject to the exception and, where applicable, their representatives, must maintain a record of all processing operations under their responsibility (*Article 30(1), GDPR*). This record must, at least, include the following:

- The name and contact details of the controller, or any joint controller or processor, and of the representative, if any.
- The name and contact details of the DPO, if any (see *Flowchart, Do we need a data protection officer?*).
- The purposes of the processing.
- A description of categories of beneficiary and of the categories of personal data relating to them.
- The recipients of the personal data. This includes the controllers to whom personal data is disclosed, including recipients in third countries or international organisations.
- Where applicable, transfers of data to a third country or an international organisation, including the identification of that country or international organisation. In the case of transfers that include one-off or infrequent processing of limited amounts of personal data in the legitimate interest of the trustee, PR or processor, the appropriate safeguards must also be documented (*Article 49(1), GDPR*).
- Where possible, a general indication of the time limits for erasure of the different categories of data.
- The description of the technical and organisational security mechanisms the trustee or PR has in place to protect data.

#### Obligations of the data processor

Data processors not subject to the exception must maintain a record of all categories of processing activity carried out on behalf of the trustee or PR (*Article 30(2), GDPR*). This includes the following information:

- The name and contact details of all the trustees or PRs for whom they are acting and of the controller's representative (if any).
- The name and contact details of the processor's DPO (if any).
- The categories of processing carried out on behalf of each controller.
- Where applicable, the categories of transfers of personal data to a third country or an international organisation.
- Where possible, a general description of the data security measures put in place by the processor. This could be satisfied by explaining that the processor is compliant with relevant professional standards such as the STEP Code for Will Preparation, the Law Society's Wills and Inheritance Quality Scheme or Law Society guidance on file retention: wills and probate and in relation to trusts.

#### Exceptions

The document requirement does not apply to controllers and processors that employ fewer than 250 persons unless at least one of the following applies to them:

- The processing they carry out is likely to result in a risk to the rights and freedoms of beneficiaries.
- The processing is not occasional.
- The processing includes special categories of personal data (see *Special category data*).

(*Article 30(5), GDPR*.)

However, regardless of the potential availability of exceptions, trustees and PRs are likely to want to maintain comprehensive and up-to-date records in compliance with their fiduciary obligations.

#### Risk to data subjects' rights and freedoms

Trustees, PRs and their professional advisers will need to evaluate what risks might be involved when they process beneficiaries' personal data. The sort of risk involved may include a risk of identity theft, fraud, financial

loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or unauthorised reversal of pseudonymisation (for a discussion of the definition, see *Practice note, Data security under the GDPR*).

The likelihood and severity of the risk must be determined by reference to the nature, scope, context and purposes of the processing (*recital 76, GDPR*). Although many of these risks will not arise in the context of trusts and estates, trustees, PRs and their professional advisers should be aware of what risk is involved when weighing up whether their efforts to keep data secure are sufficient.

**Data protection by design and by default**

Trustees and PRs are obliged to implement data protection measures "by design and default" when processing beneficiaries' personal data (*Article 25(1), GDPR*). This means that they must implement appropriate compliance systems and processes to ensure compliance with data protection principles.

When doing this they should take into account:

- What technological aids are available to them.
- The cost of implementing any systems.
- The nature, scope, context and purposes of processing.
- What risks to beneficiaries are involved.

Data controllers must take measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed (data minimisation) (*Article 25(2), GDPR*). That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility. In particular, the measures they take should prevent unauthorised sharing of beneficiary data with third parties.

**Data security**

Trustees, PRs and their professional advisers must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the beneficiary data to be protected (*Article 32(1), GDPR*).

They must ensure that anyone acting under their authority who has access to the personal data does not process it except on their instructions (*Article 32(4), GDPR*).

**Security measures**

Measures trustees, PRs and their professional advisers may take include:

- The pseudonymisation and encryption of personal data (for more information, see *Practice note, Data security under the GDPR*). (Pseudonymisation and encryption do not stop the data being personal data for GDPR purposes. They are measures to reduce the risk of breaches and harm to individuals if there is a breach. By contrast, anonymised data is not personal data subject to the GDPR.)
- Making sure processing systems are robust enough to provide ongoing confidentiality and integrity.
- Putting disaster recovery policies in place so that personal data can be accessed or restored quickly if there is a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(*Article 32(1), GDPR.*)

These measures are partly reflective of the drivers of the GDPR to move with the times in the area of cyber resilience. Trustees and PRs should use proportionate measures to safeguard personal data they hold. At the very least, this requires a recognition that what may have been adequate when the DPA 1998 came into force may not be sufficient under the new regime.

**Data security breach**

Trustees and PRs must notify any personal data breach to their national supervisory authority (in the UK, the ICO) and, in certain instances, the data subject. Data processors acting for trustees and PRs must report any data security breaches to the trustees or PRs for whom they act.

**Notification to supervisory authority**

Trustees and PRs are required to notify breaches to the ICO without undue delay and in any event within 72 hours of becoming aware of them (*Article 33(1), GDPR*). Processors must inform their controller "without undue delay after becoming aware" of a breach (*Article 33(2), GDPR*).

Processors acting for trustees and PRs do not, however, have to notify the ICO about breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons".

There are detailed formal requirements for the notification to a supervisory authority. The notification must at least:

- Describe the nature of the personal data breach, including the categories and number of data subjects concerned, and the categories and approximate number of data records concerned.
- Communicate the identity and contact details of the DPO or other contact point where more information can be obtained.
- Describe the consequences of the personal data breach.
- Describe the measures proposed or taken by the controller to address the personal data breach.

(*Article 33(3), GDPR.*)

The trustee or PR must document any personal data breach, including its effects and any remedial action taken (*Article 33(5), GDPR*).

**Notification of data subjects**

If the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller must also tell the data subject without undue delay (*Article 34(1), GDPR*).

The beneficiary must be told, in clear and plain language, the nature of the personal data breach and, at least:

- The identity and contact details of any DPO or other contact point where more information can be obtained.
- The consequences of the personal data breach.
- The measures proposed or taken by the trustee or PR to address the personal data breach.

(*Article 34(2), GDPR.*)

There is no need to inform beneficiaries of the breach if any of the following apply:

- The trustee or PR has implemented appropriate technical and organisational protection measures (for example, by encrypting data), and those measures were applied to the personal data affected by the breach.
- The trustee or PR has followed up the breach with measures which ensure that the high risk to the rights and freedoms of beneficiaries is no longer likely to materialise.
- It would involve disproportionate effort (but this can only be used as a reason where the trustee or PR can use a public communication or other measure to inform the beneficiary instead).

## ICO's sanction powers

Currently, the maximum fine that the ICO can impose on data controllers for breaching data protection requirements is £500,000. This will be significantly increased under the GDPR. The sanctions regime will also be extended to data processors.

The GDPR allows fines to be imposed as follows:

- Up to EUR10 million or, in the case of an undertaking, up to 2% of annual worldwide turnover of the preceding financial year (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notifications, DPOs and data protection by design and default.
- Up to EUR20 million or, in the case of an undertaking, 4% of annual worldwide turnover of the preceding financial year (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subject rights and international data transfers.

(*Article 83, GDPR.*)

It is not clear how the percentage fine, applied to the turnover of an "undertaking", might apply to trustees and PRs. It is likely that when fines are imposed on parties that are not an "undertaking", their economic

situation will be taken into account (recital 150, GDPR). However, the possibility of fines will focus the minds of trustees, PRs and their professional advisers on compliance. In practice, if the ICO were to impose a penalty, and trustees or PRs considered it to be disproportionate, they could take court action to challenge the amount.

Trustees, PRs and data controllers employed by them may have to compensate beneficiaries for damages where the GDPR has not been complied with or where data has not been processed in line with the trustees' or PRs' lawful instructions (Article 82, GDPR).

For more information, see *Practice note, EU General Data Protection Regulation: enforcement, sanctions and remedies.*

## HOW CAN TRUSTEES AND PRS PREPARE FOR THE GDPR?

There are many steps that trustees will need to take to prepare for the GDPR and it is unlikely that their current arrangements are GDPR-compliant. Some of the requirements of the GDPR will become clearer when regulatory guidance is finalised. In the meantime, trustees can begin to prepare, for instance, by reviewing their current arrangements and the data they hold, putting in place new processes (particularly around the reporting of personal data breaches) and reviewing processes, systems and documents. All of this will take time, so trustees should plan now what steps they need to take to be able to comply with the new regime from May 2018. Furthermore, GDPR compliance should not be considered a one-off exercise to ensure compliance by 25 May 2018. Rather, the ICO and other supervisory authorities will want to be satisfied that GDPR compliance is internalised and reflected in the way data controllers and processors carry out their activities on a dynamic basis over time.

### Possible action plan for trustees and PRs

Some of the key action points trustees and PRs may want to consider are:

- Decide which individual trustees or PRs will deal with GDPR compliance; for instance, nominate one of the trustees or PRs as the main point of contact for beneficiary requests for information.
- Assess whether the requirement to appoint a DPO applies (in most cases, probably not; see *Flowchart, Do we need a data protection officer?*). Be aware that voluntarily appointing a DPO (or someone with an equivalent job title) may inadvertently attract GDPR obligations where this is not intended.
- Regularly assess progress (for example, by including GDPR compliance as a standing item on the agenda at trustee meetings).
- Conduct an audit of personal data (including, but not limited to, beneficiary data) currently held, including:
  - where and how long it is held for;
  - reasons for the decision to keep the data for a specific time (for example, the trust period is 125 years, the estate administration is likely to take five years to complete, or taking into account the limitation periods within which further legal claims could be made);
  - who it relates to (for example, trustees who only keep data about identifiable beneficiaries and do not concern themselves with tracking down beneficiaries who are unlikely ever to benefit);
  - why it is being processed (that is, the lawful for each processing activity they will rely on, such as compliance with a legal obligation); and
  - how it is kept secure.
- Consider who the data is shared with.
- Identify whether any data held could fall within "special categories of data" (see *Special category data*).
- Consider how long the data is to be kept. The GDPR requires trustees to keep data for "no longer than is necessary for the purposes for which the personal data are processed ..." (Article 6(1), GDPR). Trustees and PRs may need to keep beneficiary data for a relatively long time. Trustees and PRs need to consider whether their policy on the storage of beneficiary data needs updating. This will also apply to professional advisers who should review their file and document retention policies.
- Assess what processing activities they currently carry out (and may carry out in the future) and identify the relevant legal ground(s) that they intend to rely on for each particular processing activity. Identifying the legal

grounds for processing is important. Data controllers are required to state the relevant processing ground in the notice provided to beneficiaries. In addition, beneficiaries' rights in relation to their personal data differ depending on which ground is relied on for its processing.

- Consider whether any changes are required to documents that are used to obtain personal data from beneficiaries (such as a requirement to communicate address or name changes).
- Update any existing data protection policies or policies about confidentiality to make them GDPR compliant. If no data protection policy exists, trustees and PRs should create one to satisfy their accountability obligations. The data protection policy should refer to:
  - the timeframe for complying with beneficiary information requests and the right to be forgotten (if relevant);
  - how they process personal data; and
  - the procedures and policies they have in place to comply with the GDPR.
- Put in place a procedure to identify, record, and if required, report, a personal data breach. This should include specific steps to be taken in the event of a breach and who is responsible for taking these steps; this may need liaison between trustees, PRs and data processors acting for them.
- Review and update procedures for dealing with data subject access requests to ensure that they meet the GDPR requirements and timelines. The controller is obliged to respond to requests from the data subject without undue delay and, at the latest, within one month and to give reasons where the controller does not intend to comply with any such requests.
- Consider whether a data protection impact assessment is required (this may be unlikely). For more information on data protection impact assessments, see *Practice note, Data protection impact assessments under the GDPR.*
- Develop and implement systems to ensure that the trustees can comply with the new requirement to report data breaches to the ICO within 72 hours.
- Create a risk register to record potential weaknesses in security systems or details of beneficiaries who may be particularly at risk if their data is leaked.
- Carry out trustee and PR training, as well as training for data processors (before 25 May 2018 if possible). Incorporate the need for training for new trustees who may be appointed after the initial training. In particular, all individuals involved in processing should be able to identify when there has been a personal data breach and be aware of how this should be dealt with.
- Review contracts with data processors to make sure they comply with GDPR requirements and agree any necessary amendments. Few existing contracts are likely to be GDPR compliant. Standard GDPR-compliant clauses published by the government may be of assistance as a starting point when reviewing contracts (see *Crown Commercial Service: Procurement Policy Note: Changes to Data Protection Legislation and General Data Protection Regulation: Action Note PPN 03/17 (December 2017)*).
- Trustees and PRs currently negotiating contracts with data processors should "future-proof" the terms to comply with the GDPR if the contractual period continues beyond May 2018.
- Data processors will have direct liability for data breaches under the GDPR and it is possible that they will seek indemnities from trustees or PRs for fines caused by the trustees' or PRs' actions. Trustees and PRs will need to consider how they approach any renegotiation of contractual terms.
- Review trustee and PR liability insurance policies to see if they can be extended to cover liability for fines and compensation under the GDPR.
- Review policies on trustee indemnities on retirement to ensure that liabilities in relation to the GDPR are taken into account.
- Engage with all data processors to ensure that GDPR obligations will be complied with and that all parties are aware of who is responsible for what.

For a toolkit containing key resources to assist trustees, PRs and data processors acting for them to prepare for and comply with the GDPR, see *EU General Data Protection Regulation toolkit.*

### Key rights of beneficiaries as data subjects

The table below lists some of the key rights beneficiaries have as data subjects:

| Right | GDPR Article |
|---|---|
| **Right to withdraw consent** to data processing (if legal ground for processing data is that beneficiary has consented). | *Article 7(3), GDPR* |
| **Right to access data.** | *Articles 14 and 15, GDPR* |
| **Right to rectification** (where data inaccurate). | *Article 16, GDPR* |
| **Right to have data erased** ("right to be forgotten") if processing no longer necessary, consent is withdrawn, beneficiary objects to processing, or processing is unlawful. Right is limited if data controller needs to keep data to comply with a legal obligation or in relation to establishing or defending a legal claim. | *Article 17, GDPR* |
| **Right to restrict processing** where beneficiary says it is inaccurate, processing is unlawful, data no longer needed, or, where legitimate interests of trustee or PR have been used as the legal ground for processing, beneficiary objects to processing. | *Article 18, GDPR* |
| **Right to transmit data to another controller** ("data portability"). This only applies where processing is automated or when the beneficiary has supplied the data **and** consent is the legal ground. | *Article 20, GDPR* |
| **Right to object to processing** (only applies where trustee or PR uses lawful ground that processing is in public interest or in exercise of official authority **or** that processing is in trustees' or PRs' legitimate interests). | *Article 21, GDPR* |
| **Right to complain to ICO** if beneficiary considers processing infringes GDPR. | *Article 77, GDPR* |
| **Right to judicial remedy** against controller or processor if beneficiary considers rights under GDPR have been infringed. | *Article 79, GDPR* |
| **Right to compensation** from controller or processor for material or non-material damage. (Controller and processor will be jointly and severally liable (*Article 82(4), GDPR*).) | *Article 82, GDPR* |

### Key obligations of data controllers and data processors

The table below lists some of the key obligations that apply to trustees and PRs as data controllers and (in some cases) to data processors acting for them:

| Obligation | Applies to |
|---|---|
| Provide beneficiaries with specified information about the personal data being processed and reasons for processing (*Articles 13 and 14, GDPR*). | Controllers. |
| Where beneficiary has asked for data to be rectified or erased, notify those with whom personal data has been shared (*Article 19, GDPR*). | Controllers. |
| Implement technical and organisational measures (policies) to ensure and demonstrate processing is performed in accordance with the GDPR (*Article 24, GDPR*). | Controllers and processors. |
| Implement processes to ensure data is safeguarded (pseudonymisation and data minimisation) (*Article 25, GDPR*). | Controllers and processors. |
| Joint controllers: determine respective responsibilities for compliance (such as who will be the point of contact when dealing with requests of information from beneficiaries) (*Article 26, GDPR*). | Controllers. |
| Ensure data processing delegated to a processor is subject to a contract that satisfies GDPR requirements such as data security and confidentiality (*Article 28, GDPR*). | Controllers and processors. |
| Maintain a record of processing activities for which they are responsible (Article 30, GDPR). | Controllers and processors. |
| Co-operate with the relevant supervisory authority (the ICO) (*Article 31, GDPR*). | Controllers and processors. |

| | |
|---|---|
| Ensure data is processed securely (*Article 32, GDPR*). | Controllers and processors. |
| Notify controller of any personal data breaches (such as accidental or unlawful destruction, alteration or unauthorised disclosure) (*Article 33, GDPR*). | Processors. |
| Notify personal data breaches (such as accidental or unlawful destruction, alteration or unauthorised disclosure) to the ICO without undue delay where breach is likely to cause risk to rights and freedoms of beneficiaries (*Article 33, GDPR*). | Controllers. |
| Tell beneficiaries about personal data breaches if likely to result in a high risk to their rights and freedoms (*Article 34, GDPR*). | Controllers. |
| Where a large amount of data is going to be processed or new technologies are involved in the processing **and** the processing is likely to result in a high risk to rights and freedoms of beneficiaries, carry out a data protection impact assessment before processing (*Article 35, GDPR*). (This is unlikely to apply in the context of private trusts and estates.) | Controllers. |
| Where a large amount of data is routinely processed, designate a data protection officer (this is unlikely to apply in the context of private trusts and estates but may, in some contexts, apply to data processors acting for trustees and PRs (see *Flowchart, Do we need a data protection officer?*)) (*Article 37, GDPR*). | Controllers and processors. |
| Where personal data is transferred to a country outside the EEA (a third country) or to an international organisation, ensure that European Commission has confirmed recipient country has adequate level of protection or, if there is no confirmation, provide appropriate safeguards (such as encryption of data) (*Articles 45 and 46, GDPR*). This obligation can be waived with the consent of the beneficiary (*Article 49(1)(a), GDPR*). (If the UK is not a member of the EEA after it leaves the EU (as is current UK government policy), it will become a third country.) | Controllers and processors. |

### Example 1: are trustees or PRs data controllers?

Alice and Brenda have been appointed executors under the terms of Aunt Caroline's will. Aunt Caroline has left her entire estate to the Royal Society for the Protection of Birds (RSPB). Alice and Brenda are not data controllers in relation to the RSPB as they do not control personal data. This because the RSPB (which is not an individual) is not a data subject. The GDPR does not apply to Alice and Brenda when they administer Aunt Caroline's estate.

However, Denis and Flora are executors of Aunt Geraldine's will which provides for all her assets to be held as an endowment fund. The fund is to provide bursaries to students studying Sanskrit at the university where the testator was a professor for many years. Denis and Flora have also been appointed as trustees of the endowment fund. Every year they receive grant applications from students who give their name, address and brief details of their studies as well as a personal statement in support of their application. The GDPR applies to Denis and Flora as data controllers in relation to the personal data they hold about the student applicants (past and present) who are data subjects. This is regardless of whether the data is contained in a computer system, on emails, or in a paper filing system.

Daphne and Fred are executors of Uncle George's will. He has left small cash gifts to all his grandchildren and the remainder of his estate to his three children. There is a provision substituting his children's spouses or civil partners as beneficiaries should any of his children predecease him. Daphne and Fred are data controllers in relation to the personal data (such as the names and addresses of all children, spouses and civil partners and grandchildren) they hold.

### Example 2: assessing what personal data is held and when to limit it

Henry and Isobel are trustees of the Jeffries Family Discretionary Trust. The settlor is Kenneth Jeffrey who defined the discretionary class as the lineal descendants of his father and mother and their spouses. Kenneth has written a letter of wishes indicating that he would like his four children and their children to be the principal beneficiaries and that the other members of the discretionary class should only benefit if his children and grandchildren have all died. He does not envisage that any other beneficiaries will ever benefit. Rather than employing a genealogical researcher to track down all Kenneth's second cousins (who he believes are settled in Queensland, Australia), the trustees decide to limit their record keeping to Kenneth's immediate family. This complies with the purpose

limitation and data minimisation principles of the GDPR. The trustees ask Kenneth to keep them informed if any of his children or grandchildren move house or get married. After Kenneth dies, they contact all Kenneth's children and grandchildren (using a privacy notice) and ask them to let them know if any of their personal details change. They have to gather this personal information to comply with their obligations to register the trust with HMRC's Trust Registration Service in any case. If all Kenneth's children and grandchildren were to die, the trustees would have to reconsider their policy about what data they process.

### Example 3: processing special category data

In his will Leonard gave his second wife, Mandy, a right to occupy his home for life. The will states that the right to occupy will terminate if Mandy remarries or cohabits. On termination of the right to occupy, the property passes to Leonard's three children from his first marriage. Leonard's PRs suspect that Mandy is cohabiting with her friend Norman. They employ a private detective to investigate Mandy's activities. Leonard's daughter has already passed on evidence that Norman is living with Mandy at the house. The PRs decide that processing the information about Mandy's sex life, although it is special category data, is justified to protect the rights of Leonard's children. However, it could be argued that hiring a detective to gather the information is not proportionate and wrongfully intrudes on Mandy's rights and freedoms.

Oscar established a life interest trust for his wife. On her death the trust assets are to be distributed to his grandchildren (excluding stepchildren and illegitimate children). Oscar has obtained information from his his daughter-in-law that indicates that one of his grandchildren is not genetically linked to him. The trustees distribute the trust fund but exclude the grandchild from benefit. The grandchild challenges the trustees' decision and requests that they disclose what data they hold about him. The trustees argue that they were holding the genetic data to enable them to distribute the trust fund according to the terms of the trust deed. The grandchild lodges a complaint with the ICO. To be consistent with the accountability principle, the trustees will want to make sure that they have a robust explanation for their actions and appropriate records, including their reasoning, as to the lawful basis for processing.

### Example 4: data subject access requests

Quentin and Roger are trustees of the Taylor Family Discretionary Trust. One of the reasons for establishing the trust was that the settlor feared that his son, Unwin, might gamble away his inheritance. The settlor wrote a letter of wishes giving details of Unwin's activities and patterns of behaviour (including details of previous criminal convictions for possession of drugs). The letter asks Quentin and Roger to treat Unwin's sister, Xan, and her children, as the primary beneficiaries and that Unwin should only benefit if there is evidence that he has mended his ways. Unwin sends Quentin and Roger a data access request which they refuse on the grounds that they suspect Unwin will make a breach of trust claim against them. They are adamant that Unwin will not receive anything from the trust fund as he shows no signs of changing his lifestyle. Quentin and Roger argue that, if they provide full details to Unwin (including their deliberations about his lifestyle), this is likely to render impossible or seriously impair the achievement of the objectives of the data processing (that is, making trustee decisions) (Article 14(5)(b), GDPR). The court subsequently needs to consider whether to order Quentin and Roger to give Unwin details of the information they hold about him. This will include consideration of whether details of their deliberations at trustee meetings should be disclosed. These deliberations, inasmuch as they contain statements of opinion, are also personal data. The court would have to balance Unwin's right to the underlying information against the effective making of trustee decisions (where, arguably, free and candid discussion might be compromised if there were a risk of disclosure). Article 7(1) of the Law Enforcement Directive ((EU) 2016/680) (which is also being implemented under the DPA 2018) applies to competent authorities and processing for law enforcement (criminal) purposes, but confirms that personal data can be based on personal assessments.