Guidance note

EU General Data Protection Regulation

Contents
Introduction
Guidance note aims and structure
Summary
Data basics
Dealing with individuals
Governance and risk management
Concluding remarks
Appendix 1 – Enforcement and sanctions
Appendix 2 – Legislative background and cross-references

November 2017
Introduction

On 25 May 2018, the EU General Data Protection Regulation (‘GDPR’ or ‘the Regulation’) will come into force, without the need for national laws to implement its provisions.

The GDPR is the result of years of negotiation, drafting and consultation. It requires greater transparency from those who handle personal data, and provides enhanced rights for individuals in respect of their information. It also raises the profile of data protection by introducing stronger sanctions for breaches.

The GDPR applies to:

- **controllers** – the person or body that determines the purposes and means of processing personal data, either alone or jointly with others; and
- **processors** – the person or body that processes personal data on behalf of the controller.

Both EU and non-EU bodies need to be aware of the GDPR because it covers:

- organisations operating within the EU;
- organisations outside the EU that offer goods or services (for payment or free of charge) to individuals within the EU; and
- organisations outside the EU that ‘profile’ individuals within the EU – i.e. use automated monitoring and analysis of a person’s circumstances, behaviour or preferences.

For ease of reference, this guidance has been drafted using corporate terminology – ‘board’, ‘directors’, ‘company secretary’ and so on. However, the GDPR applies to organisations of all kinds and across all sectors.
Guidance note aims and structure

Decision-makers at the highest levels will need clear, reliable updates from those more closely involved in the management of data throughout the organisation. Input will be required from multiple functions including legal, HR, IT and other departments such as customer services and marketing.

Company secretaries can act as a conduit for this information – helping the board raise appropriate questions of management, and assisting respondents by highlighting important or missed considerations.

This guidance note provides an overview of the new legal landscape, and the strategic and practical considerations raised by the GDPR. More detailed support is provided in boxes throughout the note:

- **Have you checked…?**
  Further information about the requirements that could act as a checklist for those closer to detail of implementation.

- **For example…**
  Examples of how practical considerations could be addressed within your organisation.

Company secretaries can also assist with the implementation of data protection measures by supporting the relevant committees tasked with oversight and helping to structure the flow of communication to the board. Possible approaches are discussed at the start of the governance and risk management section on page 26.

Cross-references to the relevant provisions of the Regulation are available in Appendix 2.

Acknowledgement

This guidance note has been prepared with the assistance of a working group comprised of ICSA members and Baker & McKenzie LLP.
Summary

<table>
<thead>
<tr>
<th>Accountability principle</th>
<th>New to the GDPR, the accountability principle requires organisations to be able to objectively demonstrate their overall compliance with the principles of the Regulation. This overarching requirement will make it even more important to have well-documented procedures that genuinely embed data protection into the way the organisation functions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data basics</td>
<td>Key to GDPR compliance is a detailed understanding of data flows throughout the organisation.</td>
</tr>
<tr>
<td></td>
<td><strong>What information do you have?</strong></td>
</tr>
<tr>
<td></td>
<td>The Regulation defines ‘personal data’, and applies enhanced rules to sensitive data (referred to by the Regulation as ‘special categories’ of data), data relating to children and profiling.</td>
</tr>
<tr>
<td></td>
<td><strong>Why do you have it?</strong></td>
</tr>
<tr>
<td></td>
<td>Organisations need to justify data collection and processing on the basis of one or more lawful grounds set out in the Regulation. The basis chosen has implications for the kinds of rights individuals can assert over the data.</td>
</tr>
<tr>
<td></td>
<td>The GDPR principles of purpose limitation, data minimisation and storage limitation also require being clear on why data has been collected, because processing activities should not be in excess of what the purpose requires.</td>
</tr>
<tr>
<td></td>
<td><strong>With whom do you share it?</strong></td>
</tr>
<tr>
<td></td>
<td>As a protective measure to prevent individuals’ rights being compromised, the GDPR makes it unlawful to transfer data to third countries or international organisations outside the EU, unless certain conditions are met.</td>
</tr>
</tbody>
</table>
The GDPR requires greater transparency from those who handle personal data, and provides enhanced rights for individuals in respect of their information.

Organisations will need to review their consent and privacy notices, as well as the effectiveness of procedures responding to withdrawals of consent and requests for information, access, erasure, restrictions to processing and rectification, as well as objections and the transfer of data to other services on behalf of individuals (portability).

Individuals also have rights in relation to profiling and automated decision making.

Data usage now pervades the way most organisations operate, and the GDPR introduces stronger sanctions for a range of potential missteps. Data protection therefore constitutes a significant risk area for organisations.

Consequently, robust governance will be necessary to ensure that data protection is integral to the way the organisation operates and that breaches are dealt with appropriately. Awareness will need to be raised across the organisation, so that all employees are clear on their responsibilities and reporting obligations.

Practical action should be taken to strengthen:

- processing arrangements;
- data protection by design and default;
- the use of Data Protection Impact Assessments;
- the role of the data protection officer; and
- compliant breach notifications.
Data basics

The GDPR applies different levels of protection to different types of data, so the extent to which your organisation is impacted upon will depend on the type of data you hold and the way you use it.

Somewhere within the organisation, someone should know and have a record of what personal data is held, where it came from and why, and with whom it is shared. An information audit may need to be carried out to achieve an appropriate level of clarity. This will provide the foundation for further compliance – for example, facilitating the ability to rectify data if requested, and enabling you to ask others to whom the data has been transferred to do the same.

Understanding your data

The Regulation protects:

- **Personal data** – any information relating to an identified or identifiable natural person (‘data subject’ – also referred to in this guidance as individual(s)). This includes information that can be used to directly or indirectly identify an individual, such as an ID number, location data, online identifier, or other factors relating to their physical, physiological, genetic, mental, economic, cultural or social identity.

- **Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic or biometric data for the purpose of uniquely identifying an individual, and data concerning an individual’s health, sex life or sexual orientation.

The GDPR also provides a new level of protection for children’s data. Privacy notices must be written in clear, plain language that a child will be able to understand. Organisations offering an ‘information society service’ (i.e. online service) and using consent as the basis for processing will need parental consent for under 16s – particularly where personal data is used for marketing or creating online profiles. There is some scope with the Regulation for the age of consent to be lowered by member states, provided it is not younger than 13.

The processing of data relating to criminal convictions and offences is also restricted under the GDPR.
Lawful processing

The processing of personal data must have a lawful basis. This should be determined and documented at the outset, before any processing begins. It must also be included in your privacy notice and as part of the answer to an access request.

The most appropriate basis will depend on the type of data being processed, and will have implications for the rights that data subjects can exercise over the processing operation.

*Have you checked…?*

Processing ordinary categories of personal data is lawful only if one or more of the following applies:

- processing is carried out with the consent of the data subject; or
- processing is necessary for:
  - performance of a contract with the data subject or to take steps to enter into a contract;
  - compliance with a legal obligation;
  - protecting the vital interests of a data subject or another person;
  - performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
  - the purposes of legitimate interests pursued by the controller or a third party – except where such interests are overridden by the interests, rights or freedoms of the data subject; or where the processing is being carried out by public authorities in the performance of their tasks.
Processing special categories of personal data is prohibited, unless:

- it relates to personal data manifestly made public by the data subject;
- processing is carried out:
  - with explicit consent of the data subject – except where reliance on consent is prohibited by other laws; or
  - by a not-for-profit body with a political, philosophical, religious or trade union aim – provided the processing only relates to members, former members, or those who have regular contact with the body in connection to those purposes, and provided there is no disclosure to a third party without consent; or
- processing is necessary for:
  - carrying out obligations under employment, social security or social protection law, or a collective agreement;
  - the protection of the vital interests of a data subject or another individual, where the data subject is physically or legally incapable of giving consent;
  - the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
  - reasons of substantial public interest derived from EU or member state law, where the processing is proportionate to the aim and contains appropriate safeguards;
  - preventative or occupational medicine, assessing the working capacity of an employee, medical diagnosis, providing health or social care, or managing health or social care systems on the basis of EU/member state law or on the basis of a contract with a health professional;
  - reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare, medical products and devices; or
  - archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

Processing data related to criminal offences and convictions should only be carried out ‘under the control of an official authority’ or in a way authorised by member state law with appropriate safeguards for the rights and freedoms of the data subject.
Transferring data

As a general rule, data cannot be transferred to third countries or international organisations outside the EU unless one of the following can be relied upon:

- **Commission decision** – the Commission has decided that a country, territory, sector or organisation ensures an adequate level of protection.
- **Appropriate safeguards** – the recipient organisation has put measures in place that will ensure that, after the transfer, individuals' rights remain enforceable and they will have access to effective legal remedies.

If neither of these conditions can be satisfied, a transfer may still be possible in certain circumstances (see box on page 10). The details of transfers will need to be known, understood and documented in order to ensure that they can be justified. Otherwise, organisations run the risk of such transfers breaching the GDPR and could face enforcement action as a consequence.

The same transfer rules apply to both controllers and processors.

Organisations that have establishments or target individuals in more than one EU jurisdiction will need to determine which supervisory authority is the ‘lead’ by identifying the organisation’s main establishment. This is where the organisation’s central administration in the EU is located, or the place where decisions about the purpose and means of processing are taken and implemented.

The supervisory authorities have greater enforcement powers under the GDPR (see Appendix 1), so having internal processes to stay on top of guidance and maintain timely communication will be important.
Have you checked…?

It should be noted that adequacy decisions from the Commission are subject to periodic review, and may be repealed or suspended.

The GDPR sets out appropriate safeguards capable of legitimising a data transfer:

- Binding Corporate Rules (BCRs) – agreements governing transfers made between organisations within a corporate group
- standard protection clauses that the Commission has adopted, or that the supervisory authority as adopted with the approval of the Commission
- legally binding agreements between public authorities
- compliance with an approved code of conduct or certification under an approved certification mechanism.

Other safeguards require the specific approval of the supervisory authority before they will be considered appropriate to legitimise a data transfer:

- contractual clauses between the transferring organisation and recipient
- provisions in administrative agreements between public authorities which include enforceable and effective rights for data subjects.

If it is not possible to rely on a Commission decision or appropriate safeguards, an organisation may still be able to justify the transfer on the basis of:

- consent – made with the individual's informed consent;*
- contract with individual – necessary for the performance of a contract between the individual and the organisation, or for pre-contractual steps taken at the individual's request;*

* These conditions are not available to public authorities exercising their public powers.
• **contract on behalf of individual** – necessary for the performance of a contract made in the interests of the individual;*
• **public interest** – necessary for important reasons of public interest;
• **legal claims** – necessary for the establishment, exercise or defence of legal claims;
• **vital interests** – necessary to protect the vital interests of the data subject or other individuals, where the data subject is physically or legally incapable of giving consent; or
• **public register** – made from a public register intended by national or EU law to give access to the information to everyone, or to individuals with a legitimate interest in inspecting the register.

One last residual category of permitted transfers exist under the GDPR, where none of the above conditions are met, but the transfer satisfies all of the following criteria:

• is not being made by a public authority in the exercise of public powers;
• is not repetitive – i.e. does not involve similar transfers on a regular basis;
• is necessary for the purposes of the compelling legitimate interests of the organisation, and those interests are not overridden by the interests of the individual;
• is made subject to suitable safeguards;
• relates to data from a limited number of individuals;
• the supervisory authority is informed; and
• the relevant individuals are informed of the transfer and the legitimate interests that necessitate it.

* These conditions are not available to public authorities exercising their public powers.
Dealing with individuals

The GDPR introduces enhanced rights for individuals in relation to their personal data, and organisations need to be prepared to respond to enquiries – sometimes within shorter time frames than are currently allowed.

Practical considerations need to be taken into account. For example, employees will need to know who is responsible for responding to particular types of requests, which systems should be used to locate and deal with the relevant data and what external notifications need to be made and how (e.g. if data has been transferred to a third party). Policies will be required to help respondents understand when an organisation can override an individual’s wishes, on what grounds and who within the organisation can exercise that discretion. Written communication with individuals in relation to their rights may need to be set out in template form, to ensure that all obligatory content is always included.

The mandatory content of privacy notices is also more detailed under the GDPR, in line with a stronger right to be informed. The Regulation also introduces a stricter definition of consent. Both of these developments will necessitate a review of existing notices to ensure that they comply with the GDPR, and it is likely that amendments will be required.

Privacy notices

Existing privacy notices should be reviewed to make sure that they are GDPR-compliant. Organisations will generally already inform individuals of their identity and how they intend to use the personal data they’re collecting. The GDPR requires further transparency (see box below).

Have you checked…?

Data subjects must be given the following information – both when data is collected directly from them and when their data is obtained indirectly from another source:

- identity and contact details of the controller, and where applicable the controller’s representative or data protection officer;
- purpose and lawful basis for the processing;
EU General Data Protection Regulation

- the legitimate interests of the controller or third party, where applicable;
- any recipient (or categories of recipients) of the personal data;
- details of transfers to third countries and safeguards;
- retention period or criteria used to determine the retention period;
- the existence of each data subject’s rights;
- the right to withdraw consent at any time, where relevant;
- the right to lodge a complaint with the supervisory authority; and
- if applicable, the existence of automated decision making (including the use of profiling, information about how decisions are made, and the significance and consequences of the decision making).

If data is collected directly from the data subject, they should also be told whether the provision of personal data is part of a statutory or contractual obligation, and the possible consequences of failing to provide the personal data.

If data has come indirectly from another source, the data subject should be told:

- the source from which the personal data originates and whether that source is publicly accessible; and
- the categories of personal data obtained.

Processes will also need revision to ensure the GDPR timing requirements are met:

- The information above must be given at the time data is collected directly from the data subject, or within a reasonable period of having obtained the data if it comes indirectly from a different source (i.e. within one month).
- If data is obtained indirectly and used to contact the data subject, the information requirements must be met when that communication takes place.
- If disclosure to another recipient is envisaged, the information above must be given to the data subject before the disclosure.
Consent

Consent is one of the lawful grounds on which an organisation can rely in order to justify data processing.

Under the GDPR, consent must be:

- **unambiguous** – a statement or clear affirmative action;
- **freely given** – this condition will not be satisfied if there is a clear imbalance of power between the controller and data subject, if the individual is unable to refuse or withdraw consent, or if the performance of a contract is made conditional on the consent;*
- **specific** – separate consents should be given for different processing activities, and broad consent to general processing will usually be insufficient (except in relation to scientific research where it is not possible to determine exactly what processing will take place – consent to specific purposes/areas of research is sufficient); and
- **informed** – individuals should understand the extent and purpose of the processing they are consenting to, and be aware of the identity of the controller.

Formal requirements must also be met for consent to be GDPR-compliant (see box on the opposite page).

Individuals must be able to withdraw their consent at any time, and this should be as easy for them to do as giving consent. Individuals also have greater rights over data provided on the basis of their consent – for example, an organisation would have to comply with a request for erasure if the data in question was held solely on the basis of consent that had subsequently been withdrawn.

Consent that has been obtained in the past will continue to be valid if it complies with the GDPR. However, organisations may want to review the extent to which they rely on consent and whether another lawful processing basis might be more suitable, given the ability for data subjects to withdraw consent at any time.

---

*Public authorities and employers will need to take particular care to meet the threshold of freely given consent.*
**Have you checked…?**

Formal requirements also need to be satisfied:

- Individuals must be informed of the right to withdraw consent at the time of consenting, and it must be as easy to withdraw consent as to give it.
- Consent can be given in oral or written form (including electronic) – oral form obviously presents evidential difficulties if the processing basis is challenged.
- Pre-formulated consent declarations must be intelligible, and in clear and plain language.
- Pre-formulated consent declarations must also be easily accessible and distinguishable from any other information given at the same time.
- Electronic requests for consent must not be unnecessarily disruptive to the use of the relevant services.
- Ticking a box, choosing technical settings and any other positive statement or conduct can be valid consent, but silence, pre-ticked boxes or inactivity will not be GDPR-compliant.

Special requirements protect children and special categories of data:

- ‘Explicit’ consent is required in relation to special categories of data – this is not defined by the GDPR, so existing EU and supervisory authority guidance will continue to apply.
- Parental consent may be required in relation to online services aimed at children.

Processes need to be in place to comply with a withdrawal of consent, and it should be noted that this can also give rise to a request for the right to erasure. There should be clear and effective procedures to action these requests.
Individuals’ rights

Data subjects have the following eight rights under the GDPR:

- the right to be informed;
- the right to access their own data;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object to processing; and
- the right not to be subject to automated decision making, including profiling.

Most of the rights are already available to individuals, but the Regulation strengthens them in some respects. The right to data portability is new. The rights are generally qualified – arising only when certain conditions are met, and sometimes capable of being refused.

1. The right to be informed

This requires organisations to provide ‘fair processing information’ in a way that is concise, transparent, intelligible and easy to access. This will normally be done through a privacy notice (see above), which must be written in clear and plain language and available free of charge.

2. The right to access own data

The rights under the GDPR are similar to those already in existence, and enable individuals to request access to their personal data, confirmation that their data is being processed and other supplementary information that corresponds to the information in a privacy notice (see above).

Access must be provided free of charge and without delay – at the latest within one month of receiving the request. (Note that this is shorter than the current 40 day period.)
The purpose of allowing individuals access to their data is limited to enabling them to be aware of, and verify the lawfulness of, the processing. This logic is reflected in some of the leeway granted to organisations by the GDPR:

- a time extension for dealing with complex or numerous requests – a further two months to respond, provided an explanation is given for the delay within one month;
- the ability to charge for or refuse to respond to a request that is ‘manifestly unfounded or excessive’; and
- permission to ask the requester to specify what data they require access to where organisations process large quantities of data.

If a request is refused, the individual must be told why and informed of their right to complain to the supervisory authority and seek a judicial remedy. This information must also be provided without undue delay – at the latest within one month.

**Have you checked…?**

Processes will need to cover the following:

- **ID verification** – Organisations will need to have ‘reasonable means’ of verifying the identity of the person making the request.
- **Format** – Electronic requests should be responded to in electronic format. The best practice recommendation under the GDPR is to give the requester remote access to a secure self-service system where they can directly access their information, bearing in mind any adverse impact on the rights and freedoms of other data subjects.
3. **The right to rectification**

Individuals can have data rectified if it is inaccurate or incomplete. If an organisation decides not to take action in response to a request, an explanation must be provided and the individual must be informed of their right to complain to the supervisory authority and to seek a judicial remedy.

A response must be provided within one month – an extension of two months is allowed for complex requests, provided an explanation is given for the delay within one month.

**Have you checked…?**

Procedures will need to be in place to ensure that:

- third parties who have received the data are informed of the rectifications, unless it is impossible or involves a disproportionate effort; and
- the individual has been informed of the third party recipients of their data, if requested.

4. **The right to erasure**

Individuals can request the deletion or removal of personal data where there is no good reason for processing to continue – this is evidenced by falling within one of the scenarios set out in the Regulation (see box on the opposite page). The GDPR also provides grounds for refusing a request for erasure.

Having clear documentation of the lawful basis for processing will help determine and explain when there are legitimate grounds to refuse the erasure of data. Third party recipients will also be required to erase the information, unless they can rely on one of the grounds for refusal.
Have you checked…?

The right to erasure can be asserted in one of the following circumstances:

- Processing was based on consent, and the individual withdraws that consent.
- The data was unlawfully processed.
- The data is no longer necessary in relation to the purpose for which it was originally collected or processed.
- The individual objects and there is no overriding legitimate interest for continuing the processing.
- A legal obligation requires the erasure.
- The data is processed in relation to online services provided to a child.

A request for erasure can be refused if the personal data is processed for the following purposes:

- exercising the right to freedom of expression and information;
- complying with a legal obligation, performing a public interest task or exercising official authority;
- public health purposes in the public interest;
- archiving in the public interest, scientific research, historical research or statistical purposes; or
- in relation to establishing, exercising or defending legal claims.

The procedures will also need to ensure that:

- third party recipients of data that should be erased are informed, unless it is impossible or involves a disproportionate effort;
- the individual has been informed of the third party recipients of their data, if requested; and
- organisations are especially prepared to remove data obtained from children. The GDPR states that the right to erasure ‘is relevant in particular where the data subject has given consent as a child and is not fully aware of the risks involved in the processing, and later wants to remove such personal data, especially on the internet’.
5. The right to restrict processing

Individuals have a conditional right to restrict the processing of their data (see box below). When processing is restricted, the data can be stored but no further processing can be carried out.

Have you checked…?

The right to restrict processing can be asserted in one of the following circumstances:

- The individual contests the accuracy of the personal data – in which case the restriction lasts for the time required to enable the data to be verified.
- The processing is unlawful, but the individual requests a restriction instead of erasure.
- Where the processing is carried out on the basis of the performance of a public interest task or for the purpose of legitimate interests – an individual has objected to the processing, and the organisation needs time to decide whether its legitimate grounds override the rights of the individual.
- When the organisation no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

Procedures must also ensure that:

- enough information is retained to make sure the restriction is respected in the future;
- third parties who received the data that is now subject to a restriction are informed about the restriction, unless it is impossible or involves a disproportionate effort;
- the individual has been informed of the third party recipients of their data, if requested; and
- if a restriction on processing is lifted, the individual concerned must be informed beforehand.
6. The right to data portability

This new right allows individuals to move, copy or transfer their personal data from one platform to another for their own purposes. The right only applies where all of the following conditions are met:

- The individual provided the personal data to the controller themselves.
- The processing is carried out by automated means.
- The processing is carried out on the basis of the individual's consent or for the performance of a contract.

As with access and rectification requests, a response to a request for data portability must be provided without undue delay, and within one month. A two-month extension is permitted for complex or multiple requests – provided an explanation for the delay is given within a month.

Again, a decision not to take action must be explained to the individual within one month at the latest, and they should also be informed of their right to complain to the supervisory authority and seek a judicial remedy.

Where the right to data portability arises, organisations must offer this facility securely and without hindrance to usability.
7. The right to object

There are three different categories of data processing that an individual can object to, and the scope of an organisation’s response depends on the category.

First, an individual can object to processing (including profiling) based on an organisation’s legitimate interests, the performance of a task in the public interest or the exercise of official authority. The objection must be on ‘grounds relating to his or her particular situation’. The objection must be complied with and processing stopped, unless either of the following apply:

- The controller demonstrates ‘compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject’.
- The processing is needed for the establishment, exercise or defence of legal claims.

---

Have you checked…?

The data has to be provided in a format that enables other organisations to use it, either:

- open formats – e.g. CSV files; or
- machine readable – i.e. structured so that software can extract specific elements of the data.

Other factors to be aware of include:

- any impact on the rights of others;
- the data must be provided free of charge; and
- an individual can request that the transfer is made directly to another organisation – this must be complied with if technically feasible, but there is no requirement to adopt or maintain processing systems that are compatible with other organisations.
Secondly, an individual can also object to processing for the purposes of scientific or historical research and statistics – again, if the objection is on ‘grounds relating to his or her particular situation’. The objection must be complied with and processing stopped, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Thirdly, an individual can also object to processing (including profiling) for direct marketing purposes. There are no exemptions or grounds to refuse.

**Have you checked…?**

The right to object to direct marketing is similar to the existing position, and it should be remembered that:

- individuals must be informed of their right to object at the point of first communication and in the privacy notice;
- the right to object must be ‘explicitly brought to the attention of the data subject and presented clearly and separately from any other information’; and
- objections to direct marketing must be dealt with at any time and free of charge.

More generally, if any of the processing that an individual can object to is carried out online, the right to object must also be offered and exercisable via online means.
8. Rights relating to profiling and automated decision making

The GDPR recognises the shift towards greater use of big data analytics and provides protection to individuals from the risk of potentially damaging decisions made on the basis of data without human intervention.

Individuals have a right to not be subject to a decision made on the basis of automated processing, if that decision produces a legal or similarly significant effect on them. Organisations need to ensure that in such circumstances, individuals can:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

The right does not apply to all automated decisions. In addition to the impact threshold above, the right does not arise if the decision is:

- necessary for entering into, or the performance of, a contract between the organisation and individual;
- authorised by law (e.g. for the prevention of fraud or tax evasion); or
- based on explicit consent.

Automated decisions in relation to the special categories of personal data cannot be made in relation to a child, and are only permitted in relation to adults if one of the following conditions are met:

- with the explicit consent of the individual; or
- processing is necessary for reasons of substantial public interest on the basis of EU/member state law – and is proportionate, respectful of rights and subject to safeguards.
Have you checked...?

The GDPR definition of profiling is detailed. It basically covers the automated monitoring and analysis of a person’s circumstances, behaviour or preferences, but organisations that potentially fall within its scope should take a closer look at the wording of the Regulation (see the legislative references in Appendix 1).

Appropriate safeguards must be in place for activities within the scope of the term, including:

- fair and transparent processing – giving details of the logic behind the processing, as well as its significance and potential consequences;
- appropriate mathematical or statistical procedures;
- measures to minimise risk of errors and enable inaccuracies to be corrected; and
- appropriate security arrangements.
Governance and risk management

Data usage has become a pervasive part of the way most organisations operate. Consequently, maintaining compliance in this area will require an ongoing and integrated approach, with oversight at the most senior level.

As well as addressing the specific governance points explored in this section (below), organisations should consider how oversight will be structured more generally. For example:

- Which committees will have responsibility for reviewing the detail and implementation of data protection measures?
- How often and in what way will this information be relayed to the board?
- What escalation procedures will be in place for non-routine updates?
- What criteria will be used to evaluate the effectiveness of data protection measures, and how will improvements be made?

Given the scope for greater enforcement action introduced by the GDPR, and the prevalence of data processing across different organisational functions, it makes sense for data protection to be treated as a risk. Organisations should consider how to integrate data issues into existing risk management processes, and whether to create new procedures.
At a basic level, data protection risks need to be identified, managed, mitigated and kept under review. That process should be documented.

Depending on internal resources, it might be appropriate to:

- Make someone with senior responsibility for risk analysis (e.g. chief risk officer) responsible for the inclusion of data protection in existing risk mitigation processes – consider how they will work with the data protection officer (see page 36 for more details on the role of the DPO).
- Within different areas of the organisation, designate smaller teams or individuals with responsibility for carrying out data retention, usage and transfer audits, and identifying risk areas specific to their function (e.g. data transfer and third party risks in procurement; consent risks in HR; risk of failure to comply with objections in marketing).
- Assign ownership of the implementation of mitigating measures to individuals with adequate training and authority.
- Prepare summaries of risk analysis and mitigating measures for the board – decide on the frequency of updates going forward.
- Include data protection and GDPR compliance as a standing item on risk committee agendas and agree a threshold for escalation to the board.

Effective risk management will also require a level of awareness about GDPR issues from everyone across the organisation. Training could cover:

- understanding the lawful basis for holding information;
- responding to individuals’ rights;
- security, retention and deletion of data;
- breach notifications and escalation procedures for reporting incidents;
- data flows between different countries; and
- responsibility for third party control and transfers of data.

Specific approaches to governance addressed by the Regulation are discussed below.
Accountability

The GDPR introduces a new accountability principle. It is an overarching requirement to objectively demonstrate compliance with all the other principles in the Regulation:

- **Lawfulness, fairness and transparency** – this requires compliance with one of the GDPR’s grounds for lawful processing, and clear, accessible communication to data subjects about the details of the processing.
- **Purpose limitation** – this limits the use of collected data to a specified, explicit and legitimate purpose, and any further processing must be compatible with the original purpose.
- **Data minimisation** – the data collected for processing should be only that which is relevant, adequate and necessary for the specific purpose.
- **Accuracy** – reasonable steps must be taken to keep data up-to-date, and inaccurate data must be rectified or deleted without delay.
- **Storage limitation** – data should not be kept longer than is necessary to fulfil the purpose of processing, and controllers should set time limits for erasure or periodic review.
- **Integrity and confidentiality** – this requires the prevention of unauthorised access or use of personal data, and implementing measures to protect data from accidental loss, destruction or damage.

The accountability principle essentially makes it necessary to keep an audit trail of policies and other indicators that show compliance is genuinely embedded in the way the organisation functions.

The principle should be front and centre of organisations’ whole response to the GDPR – coherently documenting data flow, processing methods, decision making, breaches, responses to individuals, allocations of responsibility and all other relevant data protection steps should become second nature.

However, there are also specific ways that the accountability principle can be observed – the Regulation mentions implementing appropriate measures, and adherence to codes of conduct or certification mechanisms.
Appropriate measures

The GDPR requires controllers to ‘implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the] Regulation’. Those measures should be reviewed and updated where necessary.

Have you checked…?

The Regulation does not give further details about the measures that should be put in place. When evaluating whether chosen measures are suitable, the GDPR requires decision makers to take a risk-based approach:

- Is the measure appropriate given the nature, scope, context and purpose of the data processing addressed?
- What risks are posed to the rights and freedoms of individuals? How severe are those risks and what is the likelihood of them occurring?

Key risks to be aware of include:

- economic or social disadvantage – including: discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality or professional secrecy, unauthorised reversal of encryptions or redaction; and
- deprivation of rights and freedoms, or obstacles to exercising control over personal data.
Codes of conduct and certification mechanisms

The GDPR endorses the creation of codes of conduct and certification mechanisms, and envisages them functioning in the following ways:

**Codes of conduct**

- purpose – to improve standards by establishing best practice
- created by trade associations and other representative bodies, with the support of government and regulators (update of existing codes permitted)
- prepared in consultation with stakeholders
- approved by the relevant supervisory authority (and the European Data Protection Board if addressing cross-border processing).

**Certification mechanisms**

- purpose – to act as a benchmark for technical and organisational measures, enabling individuals to quickly assess the level of data protection incorporated into a particular product or service
- issued by the supervisory authority, or certification bodies accredited by the supervisory authority
- valid for a maximum of three years.

Codes of conduct and certification mechanisms are both voluntary, and present a number of benefits and risks that will need to be considered when deciding whether to engage with either or both:

**Benefits**

- help organisations understand how to meet GDPR requirements, and also objectively demonstrate compliance – as required by the accountability principle
- a mitigating factor against enforcement action (if successfully adhered to)
- competitive advantage over other organisations by demonstrating data protection standards (particularly for processors attracting work from controllers).
Costs

- organisations would be subject to mandatory monitoring by a body accredited by the supervisory authority (codes of conduct)
- organisations would be required to provide all necessary information and access to processing activities to enable assessment for certification by relevant body (certification mechanisms).

Risks

The key risk is that, having signed up to the schemes, an organisation fails to adhere to the standards required by the code of conduct or certification mechanism. Consequences could include:

- withdrawal of certification, or suspension/exclusion from code of conduct – this would be notified to the supervisory authority
- administrative fine – up to €10 million or 2% of global turnover.

The Regulation states that both codes of conduct and certification mechanisms should take into account the specific needs of micro, small and medium-sized enterprises.

Processing arrangements

For most organisations, data handling will be carried out in conjunction with others. Your organisation might be classified as a controller, joint controller or processor (see Introduction for summary definitions), and it is likely that contractual relationships will exist governing your role in the processing.

The GDPR is more prescriptive about the relationship between processors and controllers, as well as sub-contracting arrangements. If a processor acts outside the scope of its authority, it will be regarded as a controller – and be subject to the relevant GDPR obligations.

Enforcement and sanctions can be brought against processors directly, as well as controllers (see Appendix 1).

Previous processing agreements are likely to need to be reviewed and updated in light of the stricter GDPR requirements.
Have you checked…?

A written processor agreement must set out the:

- subject matter and duration of processing;
- nature and purpose of processing;
- type of personal data and categories of data subjects; and
- obligations and rights of the controller.

The processor must be expressly required to:

- process personal data only on the documented instructions of the controller (unless a legal obligation requires the processor to do otherwise, in which case the controller should normally be notified first);
- ensure people processing the data are subject to suitable confidentiality obligations;
- implement security measures;
- return or delete data at the end of the processing operation (as requested by the controller);
- assist the controller in responding to requests from data subjects, the supervisory authority, and with other procedures – including DPIAs and breach notifications (see below); and
- provide all the information necessary for the controller to demonstrate its compliance with the GDPR requirements for engaging a processor.

The engagement of sub-processors must:

- be with the prior written consent of the controller;
- contractually incorporate the data protection obligations of the initial processor; and
- retain the liability of the initial processor if the sub-contractor fails to fulfil its data protection obligations.
Controllers must only use processors which provide ‘sufficient guarantees to implement appropriate technical and organisational measures’ so that processing will comply with the GDPR. Codes of conduct and certification mechanisms can be used to help demonstrate sufficient guarantees.

Both controllers and processors are also required to keep a written record of all categories of data processing activities under their respective responsibility, including details of:

- the organisation’s name and contact details, including of the DPO (if applicable) or other relevant representative;
- the purpose of processing and time-limits envisaged for erasure of data (controllers);
- descriptions of the categories of data subjects and personal data (controllers), and type of processing (processors);
- transfers of data to third countries or international organisations (controllers and processors); and
- descriptions of the technical and organisational measures for keeping data secure (controllers and processors).

Small organisations (fewer than 250 employees) are exempt from the record-keeping requirements, unless the supervisory authority considers the risks merit inclusion in the regime.
Data protection by design and default

Controllers are explicitly required by the GDPR to protect data by design and default.

Data protection by design means that whenever business practices, IT processes or physical infrastructures are conceptualised, maintaining privacy and data security must be integrated at the outset. Data protection should be integral to the operation of every process, not added on as an afterthought.

Data protection by default means that as a general rule, only the data required for a specific, identified purpose should be processed.

Have you checked…?

Steps to help implement data protection by design could include:

- ‘pseudonymising’ personal data – redaction, encryption and other measures to ensure the information cannot be attributed to a specific individual without further steps being taken;
- transparency and monitoring – being clear about why and how data is being processed and enabling the data subject to monitor processing; and
- security features – ensuring technological safeguards are used to limit access to data, as well as educating staff about how to avoid behaviours that increase the vulnerability of data.

Data protection by default involves minimising:

- the amount of data collected;
- the extent of processing activities;
- the length of time for which data is stored; and
- the number of people able to access the data.

Carrying out a Data Protection Impact Assessment could also highlight risks and prompt subsequent changes (see below).
Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is an evaluative tool to help think through the risks to individuals’ rights and freedoms that a particular type of data processing may cause. They are the responsibility of controllers, but processors are required to assist if requested.

The GDPR does not set out a specific format for these assessments – only a general indication of scope – but supervisory authority guidance can be referred to for more help.

Under the GDPR, the assessment is mandatory if the processing envisaged is likely to result in a high level of risk to the rights and freedoms of individuals. Examples are given by the Regulation, but the list is non-exhaustive:

- using new technologies
- automated processing, including profiling, leading to decisions that are likely to significantly affect the individuals involved
- large scale processing of special categories of personal data
- large scale processing of data relating to criminal convictions
- large scale systematic monitoring of publicly accessible areas

DPIAs need to be completed prior to the start of the data processing, and can address more than one project.

If, as a result of carrying out the DPIA, an organisation concludes that it cannot mitigate the risks raised, the supervisory authority must be consulted prior to processing. The supervisory authority will give further direction as to whether the processing can be carried out in compliance with the GDPR.
Have you checked…?

As a minimum, DPIAs should cover:

- a description of the processing envisaged;
- the purpose of the data processing;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risks to the rights and freedoms of the data subjects; and
- measures envisaged to address those risks – including safeguards, security and demonstrable compliance with the GDPR generally.

If consulted, the supervisory authority must be given the following information:

- outline of the respective responsibilities of controller, joint-controllers and processors if applicable (in particular for processing within a group of undertakings);
- purposes and means of the envisaged processing;
- measures and safeguards to protect the rights and freedoms of individuals;
- the contact details of the data protection officer, where applicable;
- the Data Protection Impact Assessment that triggered the referral; and
- any other information, as requested by the supervisory authority.

Role of the data protection officer

Any organisation is able to appoint a data protection officer (DPO). However, a DPO is mandatory for:

- public authorities (except courts);
- organisations that carry out large scale systematic monitoring of individuals (e.g. online behaviour tracking); and
- organisations that carry out large scale processing of special categories of data or data relating to criminal convictions and offences.
EU General Data Protection Regulation

Despite the fact that a DPO may not be strictly required by the GDPR in your organisation’s circumstances, serious consideration should be given to appointing one if the role does not currently exist. Given the ongoing importance of data protection and the need to provide a point of contact to liaise with the supervisory authority and data subjects, having an effective DPO will greatly facilitate compliance.

Organisations may also need to evaluate whether the person currently designated as responsible for data protection is best placed to fulfil the functions of the DPO, or whether an alternative appointment should be made. The GDPR envisages a level of autonomy, expertise and internal reporting that may not be met by current arrangements.

As a minimum, the DPO has responsibility for:

- informing and advising the organisation and its employees about their GDPR obligations and compliance with other data protection laws, including through training;
- monitoring compliance – including managing internal processes, advising on DPIAs and conducting internal audits; and
- facilitating the relationship with the supervisory authority and individuals whose data is processed as the first point of contact.

The DPO can have other duties outside of their data protection work, but these must be compatible with the time commitment required for the data protection tasks and not cause a conflict of interest.

The DPO must report directly to the board or highest level of decision makers in the organisation, and be given adequate resources to do their job. They must be free to act independently without being penalised for performing their tasks.

When it comes to choosing a DPO, there is some flexibility within the framework of the GDPR:

- The DPO can be an internal employee or external advisor.
- A single DPO can be appointed for a group, provided that the DPO is accessible from each organisation.
- Specific qualifications are not prescribed by the Regulation.
- Data protection expertise is required – the DPO should have sufficient professional experience and knowledge of data protection law to fulfil the minimum responsibilities of the role, proportionate to the activities of the organisation.
Breach notifications

Some organisations are already required to notify the supervisory authority when they suffer a personal data breach.

The GDPR extends this requirement to all controllers in relation to certain thresholds of data breaches, and also requires individuals to be notified in some cases.

A notification must be given to the supervisory authority within 72 hours of becoming aware of a breach, if the breach is likely to result in a risk to the rights and freedoms of individuals.

A notification must be given to the affected individuals without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of those individuals.

The kinds of potential risks envisaged include:

- discrimination;
- damage to reputation;
- financial loss;
- loss of confidentiality; and
- any other significant economic or social disadvantage.

On the wording of the legislation, there is some discretion for controllers to decide not to notify a breach to the supervisory authority, if the organisation concludes that the breach is unlikely to result in a risk to the rights and freedoms of individuals.

However, controllers would need to be able to demonstrate the basis of that conclusion (to comply with the accountability principle), and could run the risk of an administrative fine of up to €10 million or 2% of global turnover if it turns out a notification should have been made, in addition to a fine for the breach itself.

It will therefore be very important to make sure clear procedures are in place to identify a breach, evaluate the risks arising from it and make the relevant notifications within the specified time frames.
EU General Data Protection Regulation

Practical considerations should include:

- **awareness training** – making sure everyone within the organisation understands the definition of a data breach and how to respond within their sphere of responsibility;
- **risk assessment** – evaluating the types of data held (e.g. a breach involving special categories of data would pose a higher risk to relevant the data subjects), specific vulnerabilities to breach (e.g. risks arising from how the data is held, the number of people with access to it etc.), and the implications of rectifying a breach (e.g. length of time and amount of internal resource required, potential reputational damage);
- **escalation processes** – establishing clear steps for alerting senior people within the organisation to the occurrence a breach (including those responsible for making the relevant notifications and any reputation management), taking into account any practical difficulties – e.g. for international organisations, the DPO being in a different time zone to where the breach has occurred; and
- **clear responsibilities** – creating well-defined roles to avoid omissions or duplication in response to a breach, as well as appointing people to address and rectify the causes of a breach quickly.

The Regulation’s definition of a ‘personal data breach’ is wider than just data loss. It refers to ‘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’.

Processors that become aware of a breach must notify the relevant controller of the breach without undue delay.
Have you checked…?

The GDPR sets out the information that should be included in a breach notification. This includes:

- the nature of the personal data breach – including categories of individuals concerned and approximate numbers; and categories of data records involved and approximate numbers;
- name and contact details of the DPO (if applicable) or other contact point;
- description of the likely consequences of the breach; and
- description of the measures taken or proposed to deal with the breach, and to mitigate potential adverse effects.

This information can be provided to the supervisory authority in stages, if it is not possible to ascertain all of the above within 72 hours.

Where individuals are notified, the communication must be in clear, plain language and should also include information on how to mitigate potential negative impacts of the breach.
Concluding remarks

The steps taken to prepare for the GDPR should be treated as the beginning of ongoing efforts to understand and control data use within your organisation. Creating a culture of data protection, and clear processes to support compliant handling, will take commitment at every level. Organisations should try to see the Regulation as a positive opportunity to strengthen transparency and accountability, ultimately improving relationships with individuals.

The following appendices provide further details of the enforcement regime and legislative context, including brief notes on the UK Government’s Data Protection Bill 2017 and cross-references to provisions of the Regulation, for those readers who require more granular information.
Appendix 1 – Enforcement and sanctions

Under the GDPR, supervisory authorities have greater enforcement and sanction powers. The Regulation also describes in more detail than previous legislation the measures and procedures that should be followed by supervisory authorities, meaning there is little discretion for member states.

In addition to the power to impose fines for breaches of GDPR requirements (see below), supervisory authorities have investigative powers – such as the ability to request information, carry out data protection audits and access physical premises. They are also given other corrective powers besides fines, including the power to issue warnings and reprimands, the power to order compliance and to suspend or limit processing or data flows.

Individuals also have certain rights in relation to alleged infringements of the GDPR. Data subjects have the right to lodge a complaint with the supervisory authority, to an effective judicial remedy and to full and effective compensation for damage suffered.

Organisations that operate in multiple jurisdictions should note that individuals are entitled to file a claim with the supervisory authority that is the most convenient for them – particularly in the member state where they live, work or where the infringement is alleged to have taken place. This will not necessarily correspond with the jurisdiction of the organisation’s lead supervisory authority. It will mean that organisations need to be prepared to defend claims in all the member states where personal data is gathered or used.

Fines

The GDPR imposes a two-tier fine system.

Tier-one infringements are subject to administrative fines of up to €10 million or in the case of an undertaking, up to 2% of the worldwide annual turnover of the preceding financial year (whichever is higher).

Tier-two infringements are subject to administrative fines of up to €20 million or in the case of an undertaking, up to 4% of the worldwide annual turnover of the preceding financial year (whichever is higher).

More detail on tier-one and tier-two infringements is listed in the following tables.

---

1 This information has been reproduced from the publication EU General Data Protection Regulation in 13 Game Changers (2016) pages 64–65 by Baker & McKenzie LLP. Used with permission.
## Tier-one infringements

| Failure to obtain parental consent where information society services are offered to children below the age of consent (Article 8) | ✓ | ✓ |
| Failure to inform data subjects that personal information about them is ‘de-identified’ (Article 11) | ✓ | ✓ |
| Failure to adhere to data protection by design and default principles (Article 25) | ✓ | ✓ |
| Failure to comply with requirements for joint controller arrangements (Article 26) | ✓ | ✓ |
| Failure to designate a representative in the EU in case not established in the EU (Article 27) | ✓ | ✓ |
| Failure to comply with the requirements for appointing, and acting as, a processor (Articles 28, 29) | ✓ (as applicable) | ✓ (as applicable) |
| Failure to maintain adequate processing records (Article 30) | ✓ | ✓ |
| Failure to co-operate with a supervisory authority on request (Article 31) | ✓ | ✓ |
| Failure to implement appropriate security measures (Article 32) | ✓ | ✓ |
| Failure to notify data breaches as required (Articles 33, 34) | ✓ | ✓ |
| Failure to carry out DPIAs as required or consult with the supervisory authority on high-risk processing (Articles 35, 36) | ✓ | ✓ |
| Failure to appoint a DPO (if mandated) (Articles 37, 38, 39) | ✓ | ✓ |
| Failure to comply with certification requirements (Articles 42, 43) | ✓ | ✓ |
**EU General Data Protection Regulation**

<table>
<thead>
<tr>
<th>Tier-two infringements</th>
<th>Responsibility on…</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controllers</strong></td>
<td><strong>Processors</strong></td>
</tr>
<tr>
<td>Failure to comply with the basic processing principles, including conditions for consent (Articles 5, 6, 7, 9)</td>
<td>✓</td>
</tr>
<tr>
<td>Failure to comply with data subjects’ rights (Articles 12–22)</td>
<td>✓</td>
</tr>
<tr>
<td>Failure to comply with cross-border transfer principles (Articles 44–49)</td>
<td>✓</td>
</tr>
<tr>
<td>Failure to comply with any obligation adopted pursuant to member state law (Chapter IX)</td>
<td>✓ (as applicable)</td>
</tr>
<tr>
<td>Failure to allow the supervisory authority access to data and/or premises in order to exercise its investigative powers (Article 58(1))</td>
<td>✓ (as applicable)</td>
</tr>
<tr>
<td>Failure to comply with an order issued by the supervisory authority in exercising its corrective powers (Article 58(2))</td>
<td>✓ (as applicable)</td>
</tr>
</tbody>
</table>
Appendix 2 – Legislative background and cross-references

While the Government has confirmed that the UK’s decision to leave the EU will not affect the commencement of the GDPR (which comes into force prior to Brexit), it has published the Data Protection Bill (the Bill).

Similar to the GDPR, the Bill will come into effect in May 2018 and align UK law with the GDPR, demonstrating the Government’s commitment to the Regulation’s provisions and providing clarity on how the UK will exercise its discretion in areas where flexibility by member states is permitted (for example, on the processing of personal data on criminal convictions).

The Bill is crucial as the GDPR is an EU Regulation that will no longer apply to the UK once it leaves the EU. Having equivalent legislation that will remain in force post-Brexit will help to ensure a smooth transition. The UK’s supervisory authority – the Information Commissioner’s Office – has encouraged businesses not to be distracted by speculation about how the GDPR will function after the UK leaves the EU: the message for the time being is one of consistency with the European regulatory regime.

The table below sets out where the topics addressed in this guidance note are covered in the Regulation. Please note this is a high-level overview highlighting key provisions – it does not provide a comprehensive list of all relevant cross-references or topics.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Legislative reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td>Article 5(2), 24, Recital 77</td>
</tr>
<tr>
<td>Breach notification</td>
<td>Articles 33–34, 83, Recitals 85, 87–88</td>
</tr>
<tr>
<td>Children’s personal data</td>
<td>Article 8, Recitals 38, 58, 71</td>
</tr>
<tr>
<td>Codes of conduct and certification mechanisms</td>
<td>Articles 40–43, Recitals 98–100, 148, 150–151</td>
</tr>
<tr>
<td>Topic</td>
<td>Legislative reference</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Consent                                                      | Articles 4(11), 6(1)(a), 7, 8, 9(2)(a)  
Recitals 32, 38, 40, 42, 43, 51, 59, 171                      |
| Controllers                                                  | Article 4(7), 28–31  
Recitals 81–82                                                |
| Data Protection Impact Assessments (DPIAs)                   | Articles 35, 36, 83  
Recitals 84, 89–96                                              |
| Data protection officer (DPO)                                | Articles 37–39, 83  
Recital 97                                                        |
| Definitions – general provision                              | Article 4                                                           |
| Design and default                                           | Article 25  
Recital 78                                                    |
| Enforcement                                                  | Articles 58, 83  
Recitals 117, 148–150                                           |
| Lawful processing                                            | Articles 6–10  
Recitals 38., 40–50, 59                                         |
| Personal data – including special categories and data relating to crime | Articles 4(1), 9, 10  
Recital 26, 51                                                   |
| Principles                                                   | Article 5  
Recital 39                                                    |
| Privacy notices / Right to be informed                       | Articles 12–14  
Recitals 58–62                                                   |
| Processing                                                   | Article 4(2), 85–91  
Recitals 153–165                                                 |
| Processors                                                   | Article 4(8), 28–31  
Recitals 81–82                                                   |
| Profiling                                                    | Article 4(4)                                                      |
| Right of access                                              | Articles 12, 15  
Recital 63                                                        |
## EU General Data Protection Regulation

<table>
<thead>
<tr>
<th>Topic</th>
<th>Legislative reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rights related to automated decision making and profiling</td>
<td>Articles 4(4), 9, 22&lt;br&gt;Recitals 71,72</td>
</tr>
<tr>
<td>Rights related to infringement and enforcement</td>
<td>Articles 77–82</td>
</tr>
<tr>
<td>Right to erasure</td>
<td>Article 17, 19&lt;br&gt;Recitals 65–66</td>
</tr>
<tr>
<td>Right to data portability</td>
<td>Articles 12, 30&lt;br&gt;Recital 68</td>
</tr>
<tr>
<td>Right to object</td>
<td>Articles 12, 21&lt;br&gt;Recitals 69, 70</td>
</tr>
<tr>
<td>Right to rectification</td>
<td>Articles 12, 16, 19</td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td>Articles 18, 19&lt;br&gt;Recital 67</td>
</tr>
<tr>
<td>Scope of GDPR</td>
<td>Articles 2, 3,&lt;br&gt;Recitals 1, 2, 22–25</td>
</tr>
<tr>
<td>Transfer of data</td>
<td>Articles 45–46, 49, 83–84,&lt;br&gt;Recitals 103–114, 148–152, 169</td>
</tr>
</tbody>
</table>
ICSA is the chartered membership and qualifying body for professionals working in governance, risk and compliance, including company secretaries.

We seek to develop the skills, effectiveness and profile of people working in governance roles at all levels and in all sectors through:

- A portfolio of respected qualifications
- Authoritative publications and technical guidance
- Breakfast briefings, training courses and national conferences
- CPD and networking events
- Research and advice
- Board evaluation services.

Guidance notes are prepared by the ICSA policy team to support the work of company secretaries and other governance professionals working in the corporate and not-for-profit sectors, and in NHS trusts.

Guidance notes offer authoritative advice, interpretation and sample materials for the many issues involved in the management and support of boards. As such, they are invaluable for those helping their organisations to build trust through good governance.

There are over 100 guidance notes available to ICSA members at www.icsa.org.uk/guidance

The Institute of Chartered Secretaries and Administrators
Saffron House, 6-10 Kirby Street
London EC1N 8TS

November 2017