

Guide to the

General Data Protection

Regulation (GDPR)

Introduction	3
What's new	4
Key definitions	6
Principles	8
Lawful bases for processing	9
Consent	11
Individual rights	16
Right to be informed	17
Right of access	20
Right to rectification	22
Right to erasure	23
Right to restrict processing	25
Right to data portability	26
Right to object	28
Rights related to automated decision making including profiling	30
Accountability and governance	33
Contracts	34
Documentation	39
Data protection by design and default	41
Data protection impact assessments	42
Data protection officers	44
Codes of conduct and certification	46
Security	49
International transfers	50
Data breaches	53
Exemptions	56
Applications	57
Children	58

Introduction

Introduction

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

Alongside the Guide to the GDPR, we have produced a number of tools to help organisations to prepare for the GDPR:

Further Reading

 [GDPR: 12 steps to take now](#) 

External link

 [Getting ready for the GDPR checklist](#)

For organisations

What's new

We will update this page monthly to highlight and link to what's new in our Overview of the GDPR.

November 2017

The Article 29 Working Party has published [guidelines on imposing administrative fines](#).

We have replaced the Overview of the GDPR with the Guide to the GDPR. The Guide currently contains similar content to the Overview, but we have expanded the sections on Consent and Contracts and Liabilities on the basis of the guidance on these topics which we have previously published for consultation.

The Guide to the GDPR is not yet a finished product; it is a framework on which we will build upcoming GDPR guidance and it reflects how future GDPR guidance will be presented. We will be publishing more detailed guidance on some topics and we will link to these from the Guide. We will do the same for guidelines from the Article 29 Working Party.

October 2017

The Article 29 Working Party has published the following guidance, which is now included in our overview.

- [Breach notification](#)
- [Automated individual decision-making and Profiling](#)

The Article 29 Working Party has also adopted guidelines on administrative fines and these are expected to be published soon.

In the [Rights related to automated decision making and profiling](#) we have updated the next steps for the ICO.

In the [Key areas to consider](#) we have updated the next steps in regard to the ICO's consent guidance.

The deadline for responses to our draft GDPR guidance on contracts and liabilities for controllers and processors has now passed. We are analysing the feedback and this will feed into the final version.

September 2017

We have put out for consultation our draft GDPR guidance on contracts and liabilities for controllers and processors.

July 2017

In the [Key areas to consider](#) we have updated the next steps in regard to the ICO's consent guidance and the Article 29 Working Party's Europe-wide consent guidelines.

June 2017

The Article 29 Working Party's consultation on their [guidelines on high risk processing and data protection impact assessments](#) closed on 23 May. We await the adoption of the final version.

May 2017

We have updated our [GDPR 12 steps to take now document](#).

We have added a [Getting ready for GDPR checklist to our self-assessment toolkit](#).

April 2017

We have published our [profiling discussion paper for feedback](#).

March 2017

We have published our [draft consent guidance for public consultation](#).

January 2017

Article 29 have published the following guidance, which is now included in our overview:

- [Data portability](#)
- [Lead supervisory authorities](#)
- [Data protection officers](#)

Key definitions

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Further Reading

 [Relevant provisions in the GDPR - Articles 3, 28-31 and Recitals 22-25, 81-82](#) 

External link

What information does the GDPR apply to?

• **Personal data**

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

• **Sensitive personal data**

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Further Reading

 [Relevant provisions in the GDPR - Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51](#) 

External link

Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:



- “a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that:



“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Further Reading

 [Relevant provisions in the GDPR - see Article 5 and Recital 39](#) 

External link

Lawful bases for processing

- For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data.
- It is important that you determine your lawful basis for processing personal data and document this.
- Your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.
- The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1)(c) and (e):



“(c) processing is necessary for compliance with a legal obligation”;

“(e) processing 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.”

- These provisions are particularly relevant to public authorities and highly regulated sectors.
- The tables below set out the lawful bases available for processing personal data and special categories of data.

Lawfulness of processing conditions

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing 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.

6(1)(f) – Necessary for 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.

Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

Conditions for special categories of data

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) – Processing is necessary for 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 and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

- This section of the Guide will be updated in due course to include information on:
 - contract, legal obligation or vital interests;
 - public task;
 - special category data; and
 - criminal conviction data.

Further reading

 [Relevant provisions in the GDPR - Articles 6-10 and Recitals 38, 40-50, 59](#) 

External link

Consent

At a glance

- The GDPR sets a high standard for consent.
- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh consents if they don't meet the GDPR standard.
- Consent means offering individuals genuine choice and control.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and granular. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent a precondition of a service.
- Public authorities and employers will find using consent difficult.
- Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

Checklists

Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes, or any other type of consent by default.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.

- We give granular options to consent to independent processing operations.
- We have named our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that the individual can refuse to consent without detriment.
- We don't make consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.

Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We don't penalise individuals who wish to withdraw consent.

In brief

What's new?

- The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanisms.
- The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action.
- Consent should be separate from other terms and conditions. It should not generally be a precondition of signing up to a service.
- The GDPR specifically bans pre-ticked opt-in boxes.
- It requires granular consent for distinct processing operations.
- You must keep clear records to demonstrate consent.
- The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.
- Public authorities, employers and other organisations in a position of power are likely to find it more difficult to get valid consent.
- You need to review existing consents and your consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

Why is consent important?

- Consent is one lawful basis for processing, and consent (or explicit consent) can also legitimise use of special category data, restricted processing, automated decision-making or overseas transfers.
- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to substantial fines.

When is consent appropriate?

- Consent is one lawful basis for processing, but there are alternatives. If consent is difficult, you should consider using an alternative basis.
- Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate.
- If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.
- If you make 'consent' a precondition of a service, consent is unlikely to be the most appropriate lawful basis.
- Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent as it is unlikely to be freely given.

What is valid consent?

- Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.
- Consent must specifically cover the controller's name, the purposes of the processing and the types



of processing activity.

- Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
- Consent should be obvious and require a positive action to opt in.
- Explicit consent must be expressly confirmed in words, rather than by any other positive action.
- There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should you obtain, record and manage consent?

- Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand.
- Include the name of your organisation and any third party controllers who will be relying on the consent, why you want the data, what you will do with it, and the right to withdraw consent at any time.
- You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or default settings.
- Wherever possible, give granular options to consent separately to different purposes and different types of processing.
- Keep records to evidence consent – who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.
- Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Further Reading

 [Relevant provisions in the GDPR - see Articles 4\(11\), 6\(1\)\(a\) 7, 8, 9\(2\)\(a\) and Recitals 32, 38, 40, 42, 43, 171](#) 
External link

In more detail - ICO guidance

We have analysed the feedback received to our [draft consent guidance](#). A summary of the responses can be found on the [Consultations pages](#) of the website.

In more detail - Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party are due to publish guidelines on consent in 2017 and the latest

timetable is for this to be agreed and adopted in December 2017.

Individual rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This part of the guide explains these rights.

Right to be informed

At a glance

- The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice.
- It emphasises the need for transparency over how you use personal data.

In brief

What information must be supplied?

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

The information you supply about the processing of personal data must be:

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

The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓

Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data are obtained.	<p>Within a reasonable period of having obtained the data (within one month)</p> <p>If the data are used to communicate with the individual, at the latest, when the first communication takes place; or</p> <p>If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.</p>

Further Reading

 [Relevant provisions in the GDPR - see Articles 12\(1\), 12\(5\), 12\(7\), 13 and 14 and Recitals 58-62](#) 
External link

In more detail - ICO guidance

Further guidance for organisations on how to comply with 'the right to be informed' is provided in the [ICO privacy notices code of practice](#).

In more detail - Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party will publish guidance on transparency in 2017, according to its workplan.

Right of access

At a glance

- Individuals have the right to access their personal data and supplementary information.
- The right of access allows individuals to be aware of and verify the lawfulness of the processing.

In brief

What information is an individual entitled to under the GDPR?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

How long do I have to comply?

Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

How should the information be provided?

You must verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, you should provide the information in a commonly used electronic format.

The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

What about requests for large amounts of personal data?

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not include an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Further Reading

 [Relevant provisions in the GDPR - see Articles 12 and 15 and Recital 63](#) 

External link

Right to rectification

At a glance

- The GDPR gives individuals the right to have personal data rectified.
- Personal data can be rectified if it is inaccurate or incomplete.

In brief

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

How long do I have to comply with a request for rectification?

You must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Further Reading

 [Relevant provisions in the GDPR - see Articles 12, 16 and 19](#) 

External link

Right to erasure

At a glance

- The right to erasure is also known as 'the right to be forgotten'.
- The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

In brief

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

When can I refuse to comply with a request for erasure?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes;
or
- the exercise or defence of legal claims.

How does the right to erasure apply to children's personal data?

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

Do I have to tell other organisations about the erasure of personal data?

If you have disclosed the personal data in question to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if you process personal information online, for example on social networks, forums or websites, you must endeavour to comply with these requirements.

As in the example below, there may be instances where organisations that process the personal data may not be required to comply with this provision because an exemption applies.

Example

A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.

Further Reading

 [Relevant provisions in the GDPR - see Articles 17 and 19 and Recitals 65 and 66](#) 

External link

Right to restrict processing

At a glance

- Individuals have a right to 'block' or suppress processing of personal data.
- When processing is restricted, you are permitted to store the personal data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future.

In brief

When does the right to restrict processing apply?

You will be required to restrict the processing of personal data in the following circumstances:



- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

Further Reading

 [Relevant provisions in the GDPR - see Articles 18 and 19 and Recital 67](#) 
External link

Right to data portability

At a glance

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

Example

midata is used to improve transparency across the banking industry by providing personal current account customers access to their transactional data for their account(s), which they can upload to a third party price comparison website to compare and identify best value. A price comparison website displays alternative current account providers based on their own calculations.

In brief

When does the right to data portability apply?

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

How do I comply?

You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

How long do I have to comply?

You must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or you receive a number of requests. You must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where you are not taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Further Reading

 [Relevant provisions in the GDPR - see Articles 12 and 20 and Recital 68](#) 

External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published [guidelines](#) and [FAQs](#) on data portability for organisations.

Right to object

At a glance

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

In brief

How do I comply with the right to object if I process personal data for the performance of a legal task or my organisation's legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

How do I comply with the right to object if I process personal data for direct marketing purposes?

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must deal with an objection to processing for direct marketing at any time and free of charge.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

How do I comply with the right to object if I process personal data for research purposes?

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right

to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

How do I comply with the right to object if my processing activities fall into any of the above categories and are carried out online?

You must offer a way for individuals to object online.

Further Reading

 [Relevant provisions in the GDPR - see Articles 12 and 21 and Recitals 69 and 70](#) 

External link

Rights related to automated decision making including profiling

At a glance

- The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
- Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

In brief

When does the right apply?

Individuals have the right **not to be subject to a decision** when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

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

Does the right apply to all automated decisions?

No. The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

What else does the GDPR say about profiling?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;

- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

You must:

- ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences;
- use appropriate mathematical or statistical procedures for the profiling;
- implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) **must not**:

- concern a child; or
- be based on the processing of special categories of data unless:
 - you have the explicit consent of the individual; or
 - the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Further Reading

 [Relevant provisions in the GDPR - see Articles 4\(4\), 9 and 22 and Recitals 71 and 72](#) 
External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published [guidelines on Automated individual decision-making and Profiling](#). The consultation period for these guidelines will run for six weeks from 17 October 2017.

Comments should be sent to the following addresses **by 28 November 2017 at the latest**.

JUST-ARTICLE29WP-SEC@ec.europa.eu and presidenceg29@cnil.fr.

In more detail – ICO guidance

We have now analysed the responses to our [request for feedback on profiling and automated decision-making](#). A summary of the responses is available on the [Consultation pages](#) of the website.

We are currently considering whether the ICO can provide any further detail over and above the Article 29 Working Party guidelines. We will add any additional advice we are able to provide here in due course.

Accountability and governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

What is the accountability principle?

The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

How can I demonstrate that I comply?

You must:

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
 - data minimisation;
 - pseudonymisation;
 - transparency;
 - allowing individuals to monitor processing; and
 - creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.

You can also:

- adhere to approved codes of conduct and/or certification schemes. See the section on codes of conduct and certification for more detail.

Contracts

At a glance

- Whenever a controller uses a processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract.
- In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.
- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.
- Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Checklists

Controller and processor contracts checklist

Our contracts include the following compulsory details:

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

Our contracts include the following compulsory terms:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;

- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
- reflect any indemnity that has been agreed.

Processors' responsibilities and liabilities checklist

In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, a processor has the following direct responsibilities under the GDPR. The processor must:

- only act on the written instructions of the controller (Article 29);
- not use a sub-processor without the prior written authorisation of the controller (Article 28.2);
- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
- ensure the security of its processing in accordance with Article 32;
- keep records of its processing activities in accordance with Article 30.2;
- notify any personal data breaches to the controller in accordance with Article 33;

- employ a data protection officer if required in accordance with Article 37; and
- appoint (in writing) a representative within the European Union if required in accordance with Article 27.

A processor should also be aware that:

- it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;
- if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;
- if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and
- if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

In brief

What's new?

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
- These contracts must now include certain specific terms, as a minimum.
- These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors - though none have been drafted so far.
- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.
- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

When is a contract needed?

- Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place.
- Similarly, if a processor employs another processor it needs to have a written contract in place.

Why are contracts between controllers and processors important?

- Contracts between controllers and processors:
 - ensure that they both understand their obligations, responsibilities and liabilities;
 - help them to comply with the GDPR;
 - help controllers to demonstrate their compliance with the GDPR; and
 - may increase data subjects' confidence in the handling of their personal data.

What needs to be included in the contract?

- Contracts must set out:
 - the subject matter and duration of the processing;
 - the nature and purpose of the processing;
 - the type of personal data and categories of data subject; and
 - the obligations and rights of the controller.
- Contracts must also include as a minimum the following terms, requiring the processor to:
 - only act on the written instructions of the controller;
 - ensure that people processing the data are subject to a duty of confidence;
 - take appropriate measures to ensure the security of processing;
 - only engage sub-processors with the prior consent of the controller and under a written contract;
 - assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
 - assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
 - delete or return all personal data to the controller as requested at the end of the contract; and
 - submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.



Can standard contracts clauses be used?

- The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (such as the ICO) to be used in contracts between controllers and processors. However, no standard clauses are currently available.
- The GDPR also allows these standard contractual clauses to form part of a code of conduct or certification mechanism to demonstrate compliant processing. However, no schemes are currently available.

What responsibilities and liabilities do processors have in their own right?

- A processor must only act on the documented instructions of a controller.
- If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.
- In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:
 - not to use a sub-processor without the prior written authorisation of the data controller;
 - to co-operate with supervisory authorities (such as the ICO);
 - to ensure the security of its processing;
 - to keep records of processing activities;
 - to notify any personal data breaches to the data controller;
 - to employ a data protection officer; and
 - to appoint (in writing) a representative within the European Union if needed.
- If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.
- If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Further Reading

 [Relevant provisions in the GDPR - see Articles 28-36 and Recitals 81-83](#) 

External link

In more detail – ICO guidance

The deadline for responses to our [draft GDPR guidance on contracts and liabilities for controllers and processors](#) has now passed. We are analysing the feedback and this will feed into the final version.

Documentation

At a glance

- As well as your obligation to provide comprehensive, clear and transparent privacy policies (see section on Individual rights), if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.
- If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:
 - processing personal data that could result in a risk to the rights and freedoms of individual; or
 - processing of special categories of data or criminal convictions and offences.

In brief

What do I need to record?

You must maintain internal records of processing activities. You must record the following information:

- name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer);
- purposes of the processing;
- description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- retention schedules; and
- description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.



Further Reading

 [Relevant provisions in the GDPR - see Article 30 and Recital 82](#) 

External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published [guidelines on lead supervisory authorities](#)  and [FAQs on lead supervisory authorities](#) . These are intended to assist in identifying which is the lead

supervisory authority when a controller or processor is carrying out cross-border processing of personal data.

Data protection by design and default

At a glance

- Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.
- Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.
- The ICO has published [guidance on privacy by design](#). We are working to update this guidance to reflect the provisions of the GDPR. In the meantime, the existing guidance is a good starting point for organisations.

Data protection impact assessments

At a glance

- Data protection impact assessments (DPIAs) help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.
- DPIAs can be an integral part of taking a privacy by design approach.
- The GDPR sets out the circumstances in which a DPIA must be carried out.

In brief

What is a data protection impact assessment?

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.

See the ICO's [conducting privacy impact assessments code of practice](#) for good practice advice. We are working to update this guidance to reflect the provisions of the GDPR. In the meantime, the existing guidance is a good starting point for organisations.

Annex 1 of the ICO's [paper on big data, artificial intelligence, machine learning and data protection](#) contains practical advice on applying GDPR DPIA provisions in the specific context of big data analytics.

When do I need to conduct a DPIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.

- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Further Reading

 [Relevant provisions in the GDPR - see Articles 35, 36 and 83 and Recitals 84 and 89-96](#) 

External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has finalised its [guidelines on high risk processing and DPIAs](#), following its consultation.

In more detail – ICO guidance

We are currently considering whether the ICO can provide any further detail over and above the Article 29 Working Party guidelines. We will add any additional advice we are able to provide here in due course.

Data protection officers

At a glance

- The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances.
- The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO.

In brief

When does a Data Protection Officer need to be appointed under the GDPR?

Under the GDPR, you **must** appoint a DPO if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking);
or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

What does the GDPR say about employer duties?

You must ensure that:

- The DPO reports to the highest management level of your organisation – ie board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.

- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Can we allocate the role of DPO to an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests.

You can also contract out the role of DPO externally.

Does the data protection officer need specific qualifications?

The GDPR does not specify the precise credentials a data protection officer is expected to have.

It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.



Further Reading

 [Relevant provisions in the GDPR - see Articles 37-39 and 83 and Recital 97](#) 

External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published [guidelines on DPOs](#)  and [FAQs on DPOs.](#) 

Codes of conduct and certification

At a glance

- The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.
- The specific needs of micro, small and medium sized enterprises must be taken into account.
- Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.
- Adhering to codes of conduct and certification schemes brings a number of benefits over and above demonstrating that you comply. It can:
 - improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
 - provide mitigation against enforcement action; and
 - improve standards by establishing best practice.
- When contracting work to third parties, including processors, you may wish to consider whether they have signed up to codes of conduct or certification mechanisms.

In brief

Who is responsible for drawing up codes of conduct?

- Governments and regulators can **encourage** the drawing up of codes of conduct.
- Codes of conduct may be created by trade associations or representative bodies.
- Codes should be prepared in consultation with relevant stakeholders, including individuals (Recital 99).
- Codes must be approved by the relevant supervisory authority; and where the processing is cross-border, the European Data Protection Board (the EDPB).
- Existing codes can be amended or extended to comply with the requirements under the GDPR.

What will codes of conduct address?

Codes of conduct should help you comply with the law, and may cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining

parental consent);

- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

What are the practical implications?

If you sign up to a code of conduct, you will be subject to mandatory monitoring by a body accredited by the supervisory authority.

If you infringe the requirements of the code of practice, you may be suspended or excluded and the supervisory authority will be informed. You also risk being subject to a fine of up to 10 million Euros or 2 per cent of your global turnover.

Adherence to a code of conduct may serve as a mitigating factor when a supervisory authority is considering enforcement action via an administrative fine.

Who is responsible for certification mechanisms?

Member states, supervisory authorities, the EDPB or the Commission are required to encourage the establishment of certification mechanisms to enhance transparency and compliance with the Regulation.

Certification will be issued by supervisory authorities or accredited certification bodies.

What is the purpose of a certification mechanism?

A certification mechanism is a way of you demonstrating that you comply, in particular, showing that you are implementing technical and organisational measures.

A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers.

They are intended to allow individuals to quickly assess the level of data protection of a particular product or service.

What are the practical implications?

Certification does not reduce your data protection responsibilities.

You must provide all the necessary information and access to your processing activities to the certification body to enable it to conduct the certification procedure.

Any certification will be valid for a maximum of three years. It can be withdrawn if you no longer meet the requirements of the certification, and the supervisory authority will be notified.

If you fail to adhere to the standards of the certification scheme, you risk being subject to an administrative fine of up to 10 million Euros or 2 per cent of your global turnover.

Further Reading

 [Relevant provisions in the GDPR - see Articles 40-43 and 83 and Recitals 98, 99, 100, 148, 150 and 151](#) 

External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

According to its workplan, the Article 29 Working Party will produce guidelines on certification in 2017.

The Article 29 Working Party has adopted [guidelines on imposing administrative fines](#).

Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

The ICO has previously produced guidance to assist organisations in securing the personal data they hold. We are working to update existing guidance to reflect GDPR provisions and once completed, this section will expand to include this information.

In the meantime, the existing guidance is a good starting point for organisations. This is located in the [guidance index](#) under the 'security' heading.

International transfers

At a glance

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

In brief

When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

What about transfers on the basis of a Commission decision?

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Further Reading

 [Relevant provisions in the GDPR - see Article 45 and Recitals 103-107 and 169](#) 

External link

What about transfers subject to appropriate safeguards?

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;

- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Further Reading

 [Relevant provisions in the GDPR - see Article 46 and Recitals 108-110 and 114](#) 

External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

According to its workplan, the Article 29 Working Party will publish guidelines on data transfers based on binding corporate rules and contractual clauses in 2017.

What about transfers based on an organisation's assessment of the adequacy of protection?

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Further Reading

 [Relevant provisions in the GDPR - see Articles 83 and 84 and Recitals 148-152](#) 

External link

Are there any derogations from the prohibition on transfers of personal data outside of the EU?



The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;

- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Further Reading

 [Relevant provisions in the GDPR - see Article 49 and Recitals 111 and 112](#) 

External link

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Further Reading

 [Relevant provisions in the GDPR - see Article 49 and Recital 113](#) 

External link

Further reading

 [Blog: Changes to Binding Corporate Rules applications to the ICO](#) 

External link

Data breaches

At a glance

- The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority.
- In some cases, organisations will also have to report certain types of data breach to the individuals affected.

In brief

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Example

A hospital could be responsible for a personal data breach if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls.

What breaches do I need to notify the relevant supervisory authority about?

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and
 - the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a breach?

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

What should I do to prepare for breach reporting?

You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Further Reading

 [Relevant provisions in the GDPR - see Articles 33, 34 and 83 and Recitals 85, 87 and 88](#) 
External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published [guidelines on Personal data breach notification](#). The consultation period for these guidelines will run for six weeks from 17 October 2017.

Comments should be sent to the following addresses **by 28 November 2017 at the latest**.

In more detail – ICO guidance

We are considering whether the ICO can provide any further detail over and above the Article 29 Working Party guidelines. We will add any additional advice we are able to provide here in due course.

Exemptions

What derogations does the GDPR permit?

Article 23 enables Member States to introduce derogations to the GDPR in certain situations.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

What about other Member State derogations or exemptions?

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;
- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- churches and religious associations.

Further Reading

 [Relevant provisions in the GDPR - see Articles 6\(2\), 6\(3\), 9\(a\)\(a\), 23 and 85-91 and Recitals 71, 50, 53 and 153-165](#) 

External link

Applications

To assist organisations in applying the requirements of the GDPR in different contexts, we are working to produce guidance in a number of areas. For example, children's data, CCTV, big data, etc.

This section will expand when our work on this guidance is complete.

Children

At a glance

- The GDPR contains new provisions intended to enhance the protection of children's personal data.
- Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

In brief



What do I need to do if I offer online services to children?

If you offer an 'information society service' (ie online service) to children, you may need to obtain consent from a parent or guardian to process the child's data.

The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility' – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

'Information society services' includes most internet services provided at the user's request, normally for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Further Reading

 [Relevant provisions in the GDPR - see Article 8 and Recitals 35, 58 and 71](#) 
External link