Data Protection and PECR Training
Supporting notes and further reading
Module 9 : The rights of the individual part 2

Introduction

These notes are designed to set out the key points covered during module 9 of our data protection online training programme. These notes are not designed to replace the online module, but are intended to be a point of reference for your follow-up study. You may find it helpful to have these notes and the relevant legislation open whilst watching the online module:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)

This document contains:

Supporting notes

Module 9 looks at the rest of the individual rights. It covers:

- Refusing an individual's request to exercise a right
- The right to be informed
- Privacy information
- The right to erasure
- The right to rectification
- The right to restrict processing
- How data can be restricted
- Informing other organisations
- The right to data portability
- The right to object to processing
- The right to object: processing based on legitimate interests or public task
- The right to object: processing for direct marketing purposes
- The rights related to automated decision making including profiling
- What does legal effect or similarly significant effect mean?
- When a controller can take automated decisions
- Appropriate safeguards
- Automated decision making and special category data
- Automated decision making and children

Refusing an individual's request to exercise a right

The rights of the data subject are not absolute and do not apply in all situations. In addition:

- the controller might apply an exemption; and
- it might refuse a request which is manifestly unfounded or excessive.

If the controller decides not to comply with a request, it must tell the data subject why and inform them of their right to:

- complain to the ICO; and
- seek a judicial remedy, which means go to court.

It should tell the data subject of this without delay, and at the latest within one month of receipt of the request (or within the extension time). It should not wait until the last minute.

The right to be informed

Controllers must be transparent in their use of personal data, and should provide information to data subjects which includes:

- their identity and contact details;
- the purposes of the processing and the lawful basis for the processing;
- if the lawful basis for the processing is legitimate interests, an explanation of what these are;
- any recipient or categories of recipients of the personal data; and
- the existence of each of the data subject's rights.

There is a table in the guidance which lists the information which needs to be provided when the personal data is collected from individuals and when it is obtained from other sources. This reflects Articles 13 and 14.

If the controller obtains the data from another source, there are two additional pieces of information which should be provided - the categories of personal data and the source of data.

The guidance also lists exceptions where privacy information does not have to be provided to the data subject.

For example, if the data has been obtained from another source, the controller does not have to provide privacy information if this would involve a disproportionate effort.

The controller also does not have to provide an individual with privacy information they already have.

Privacy information

Privacy information must be provided to the data subject:

- at the time the data is collected;
- or, if obtained from another source, within a reasonable period of having obtained the data (this means within one month);
- if the data is used to communicate with the individual, at the latest, when the first communication takes place; or

- if disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

The information should be:

- concise, intelligible and easily accessible; and
- in clear and plain language (this is particularly important when the information is addressed specifically to a child).

The controller should:

- explain acronyms and avoid confusing terminology;
- consider the best way to communicate the information, for example, in writing or through signage; and
- use a layered approach or just in time notices, icons and symbols.

The right to erasure

The right to erasure (Article 17) enables an individual to request the deletion of personal data where there is no compelling reason for its continued processing.

The right to erasure is also known as 'the right to be forgotten'.

It is not an absolute right and applies only in specific circumstances.

These include when:

- the personal data is no longer necessary for the purpose it was originally collected for. For example, performance reviews held by your old company;
- the individual withdraws consent;
- the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- the personal data was unlawfully processed (so there has been an infringement of the UK GDPR). For example if CCTV footage was taken with no signage;
- the personal data has to be erased in order to comply with a legal obligation. For example, your fingerprint must be erased if you are found innocent of a crime; and

- the personal data is processed in relation to the offer of information society services (ISS) to a child.

If any of the above apply, the controller must erase the data if requested, unless one of the following applies and processing is necessary:

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

The right to rectification

The right to rectification (Article 16) entitles individuals to:

- have inaccurate data amended without delay; and
- have incomplete data completed, including by means of providing a supplementary statement.

A controller should take reasonable steps to satisfy itself that the data in question is accurate. It should take into account the purpose of the processing, and the arguments provided by the data subject. If it finds that the information is inaccurate, it should take reasonable steps to rectify it.

The more important it is that the data should be accurate, the greater effort should be put into taking reasonable steps.

If the controller is satisfied that the personal data in question is accurate, it should let the individual know its decision. We consider it to be good practice for the controller to place a supplementary statement on its system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

The right to restrict processing

An individual has the right to restrict processing (Article 18). It allows them to prevent further processing of their personal data where they have a particular reason for wanting the restriction.

This is not an absolute right and only applies in certain circumstances.

It has close links to the right to rectification and the right to object and applies when the data subject:

- has objected to processing; or
- has contested the accuracy of their personal data and asked for it to be rectified.

In both cases, the data subject might ask the controller to restrict the processing while it considers the objection or request for rectification. It's good practice for the controller to automatically restrict the processing while it considers the reasons for the request. Once the controller has made its decision, it may decide to lift the restriction and it must inform the individual before it does so.

The right to restriction also applies when:

- the controller doesn't need the data anymore but the data subject requires it for legal claims.
- the processing is unlawful (an infringement of the UK GDPR) but the data subject prefers restriction to erasure. For example, if CCTV footage is obtained without a lawful basis but the data subject wants the footage retaining to prove something.

How data can be restricted

In most cases the controller will not be required to restrict an individual's personal data indefinitely but for a certain period of time.

When processing is restricted, a controller is permitted to store the personal data, but not use it.

The UK GDPR sets out the following examples of how data could be restricted (or suppressed):

- temporarily moving the selected data to another processing system;
- making the selected data unavailable to users; or
- temporarily removing published data from a website.

Where data has been restricted, a controller must not process the data in any manner except to store it unless:

- it has the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person; or
- it is for reasons of important public interest.

Informing other organisations

If the controller has disclosed the data to other organisations then it **must** inform those organisations about any erasure, restriction or rectification of that data, unless to do so:

- proves impossible; or
- involves disproportionate effort.

If requested by the data subject, the controller should inform them which organisations it has disclosed the data to. This is outlined in Article 19.

In addition, our guidance on the right to erasure says:

- when a controller is obliged to erase personal data it has made public, it must take reasonable steps to inform other controllers processing the data about the erasure.
- this includes erasure of any links to the data, or any copy or replication of the data.

When deciding what are reasonable steps, the controller can take into account available technology and the cost of implementation.

Example: a doctor records a diagnosis of depression for a patient and prescribes a specific drug as medication

- two years later the patient disputes the diagnosis and argues a different drug was prescribed. They contact the surgery and demand the entry concerning depression is erased and that the drug name is altered in the medical record. They want the practice to stop processing the data while it makes these changes

- this request involves erasure, rectification and the restriction of processing

- the practice may decide to restrict the processing of the relevant personal data while it decides how to handle the request

- the patient has argued for erasure of the diagnosis data, but this falls under rectification as the dispute is about the accuracy of the data

- although the patient disputes the medical record and claims they were never depressed, this is an accurate reflection of the doctor's opinion at the time. The practice has a legal obligation to maintain accurate medical records. There are no valid grounds for erasure

- the practice adds a supplementary statement to the medical record, to reflect the fact that the patient does not consider the diagnosis to be accurate

- with respect to the type of drug prescribed, the practice should take reasonable steps to satisfy itself that the data in question is accurate – taking into account the arguments and evidence provided by the patient

- as the drug was prescribed two years ago, the practice may argue that the accuracy of this information is not crucial and that the steps it has taken to check the record are reasonable in the circumstances

- the practice could add a supplementary note to the drug record

- the practice should explain its decision to the patient and inform them of their right to make a complaint to the ICO and the ability to seek to enforce their rights through a judicial remedy

The right to data portability

The right to data portability (Article 20) means data subjects are able to move their personal data easily between controllers in a safe and secure way, without hindering usability.

The idea is that data subjects can obtain and reuse their personal data for their own purposes across different services, for example, to switch insurance or utility providers.

The controller should provide the data either to the data subject or another controller in a structured, commonly used and machine readable form so other organisations can extract and use the data.

The right to data portability does not cover all of the data subject's personal data. It only applies to information the data subject has provided to the controller themselves. This includes account data such as mailing address, user name and age. It also includes data where there is observation of the individual's activities when using a service or device. For example, raw data processed by connected objects such as smart meters and wearable devices such as a fitness wristband.

It does not include data which has been created or inferred by the controller using observed data or data that has been directly provided, such as a user profile created by analysis of raw data collected from a smart meter.

It also only applies where:

- the processing is based on the individual's consent or for the performance of a contract; and
- is carried out by automated means.

The right to object to processing

The UK GDPR gives individuals the right to ask organisations to stop processing their data.

This right to object (Article 21) applies where processing, including profiling, is:

- based on legitimate interests or public task; and
- for direct marketing purposes.

There is also a right to object if the processing is for scientific/historical research and statistical purposes, but this right is more limited. Please see the guidance for further information.

If a controller accepts an objection to processing, it may need to erase the personal data. This will depend on the purposes for its processing.

The right to be informed requires an individual is explicitly told about the right to object.

The right to object: processing based on legitimate interests or public task

An individual can object to the processing of their personal data where processing is based on legitimate interests or public task.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

The right is not absolute and so an organisation must stop processing the personal data unless:

- it 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.

Where a controller is determining whether it has compelling legitimate grounds which override the interests of an individual, it must consider the reasons for the objection.

If the controller is satisfied that it does not need to stop processing the personal data in question, it should let the individual know.

The right to object: processing for direct marketing purposes

An organisation must stop processing personal data for direct marketing purposes as soon as it receives an objection.

This includes any profiling of data to the extent that it is related to direct marketing.

This is an absolute right and there are no exemptions or grounds to refuse. This does not automatically mean that a controller needs to erase

the individual's personal data. We recommend a controller should retain enough information about them to ensure that their preference not to receive direct marketing is respected in future.

The rights related to automated decision making including profiling

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

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

This means the UK GDPR safeguards individuals against the risk that a potentially damaging automated decision is taken about them without human involvement.

What does legal effect or similarly significant effect mean?

These types of effect are not defined in the UK GDPR; however, the decision must have a significant impact on an individual's life to be caught by this provision.

A legal effect is something that adversely affects someone's legal rights.

Similarly significant effects are more difficult to define, but could include the automatic refusal of an online credit application, and e-recruiting practices without human intervention.

The right won't apply if the decision only affects the individual in a trivial or negligible way. For example, an individual enters an online "personality quiz" and answers questions about themselves on a website, which then uses their responses to automatically generate a personality profile for them. The automated decisions on which the personality profile is based do not have a significant effect on the individual.

Another example of a trivial decision is where an individual receives recommendations for new television programmes based on their previous viewing habits.

Example: processing based on automated decision making and which would have a significant effect similar to a legal effect

- a social security process which automatically evaluates benefit claims and decides whether benefit is to be paid and if so how much, would be a decision 'based solely on automated processing' for the purposes of Article 22
- as well as having a legal effect, the amount of benefit received could affect a person's livelihood or ability to buy or rent a home, so this decision would also have a 'similarly significant effect'

Example: processing based on automated decision making and which would have a significant effect similar to a legal effect

- as part of their recruitment process, an company decides to interview certain people based entirely on the results achieved in an online aptitude test
- this decision would have a significant effect, since it would determine whether or not someone can even be considered for the job

When a controller can take automated decisions

A controller can take automated decisions including profiling if it does not have a legal or similarly significant effect.

In addition, it can carry out solely automated decision-making with a legal or similarly significant effect in certain specific circumstances – if the decision is:

- necessary for entering into, or the performance of, a contract between an organisation and the individual (for example an individual taking out a loan application involves a contract – the credit reference agency will automatically generate a credit score for the financial organisation and this is necessary for the contract to be fulfilled);
- authorised by law (for example, for the purposes of fraud or tax evasion prevention); or

- based on the individual's explicit consent.

But if this is the case, there is still another layer of protection.

Appropriate safeguards

Controllers must ensure that appropriate safeguards are in place.

The controller should:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;

- use appropriate mathematical or statistical procedures;

- ensure that individuals are able to:
    - obtain human intervention;
    - express their point of view; and
    - obtain an explanation of the decision and challenge it;

- 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.

Because this type of processing is considered to be high risk, the UK GDPR requires the controller to carry out a Data Protection Impact Assessment.

And remember, data subjects have the right to object to any processing of their personal data for direct marketing purposes, which includes profiling to the extent that it is related to direct marketing.

Automated decision making and special category data

If a controller is processing special category data it can **only** carry out automated decision making if:

- the individual has given explicit consent; or
- the processing is necessary for reasons of substantial public interest on the basis of UK law.

The controller would need to have suitable measures in place to safeguard the data subject's rights and freedoms and legitimate interests.

Automated decision making and children

The UK GDPR makes no specific reference to children and profiling, so the same basic rules apply to them as to adults.

Children have an absolute right to object to profiling that is related to direct marketing.

Our position is that a controller should not make decisions about children that are based solely on automated processing (including profiling) if these have a legal effect on the child or similarly significant affects them.

A controller should generally avoid profiling children for marketing purposes.

If a controller decides to do this, it should ensure there are suitable measures in place to protect them. It should provide clear information and not exploit any lack of understanding or vulnerability.

Example: an individual applies online for a loan to buy a car and the loan is declined

- the company tells the individual the system made the decision and that it was based on profiling
- the individual complains to the ICO who find that the processing was not compliant with the UK GDPR as it fell under automated decision making with no human involvement
- it had a significant effect on the individual and the controller has no safeguards in place
- the company argued it was able to process the automated decision because it was necessary for entering into a contract
- the controller had not proactively informed its customers about the automated decision-making process in its privacy notice. It didn't provide meaningful information about the logic involved and didn't explain the significance and envisaged consequences of the processing to the data subject

- the individual was not aware they could request human intervention, express their point of view or challenge the decision
- finally, the controller had not carried out a DPIA before it started using this system

Back to top

Further reading

The right to be informed

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right to be informed

Read the 'At a glance' points and the 'In brief' questions and answers. You should take some time to read the listed questions but in particular, look at the bottom of the list: The right to be informed in more detail.

This provides more information, including a few key questions:

- What information must we provide when we collect personal data from individuals?
- What information must we provide when we obtain personal data from another source?
- At what point do we have to provide information to individuals?
- How should we write and present the information?
- Are there different ways we can provide privacy information?

The right to erasure

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right to erasure

Read the 'At a glance' points and the 'In brief' questions and answers.

You should take some time to read the listed questions but in particular, look at:

- What is the right to erasure?
- When does the right to erasure apply?
- How does the right to erasure apply to data collected from children?
- Do we have to tell other organisations about the erasure of personal data?

Find an example of a manifestly unfounded request (see the yellow boxes for examples).

The right to rectification

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right to rectification

Read the 'At a glance' points and the 'In brief' questions and answers.

You should take some time to read the listed questions but in particular, look at:

- What is the right to rectification?
- What do we need to do?
- When is data inaccurate?
- What should we do about data that records a mistake?
- What should we do about data that records a disputed opinion?

The right to restrict processing

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right to restrict processing

Read the 'At a glance' points and the 'In brief' questions and answers.

You should take some time to read the listed questions but in particular, look at:

- What is the right to restrict processing?
- When does the right to restrict processing apply?
- How do we restrict processing?
- Can we do anything with restricted data?

The right to data portability

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right to data portability

Read the 'At a glance' points and the 'In brief' questions and answers.

Choose a few of the questions, but in particular look at:

- What is the right to data portability?
- When does the right apply?
- What does the right apply to?

- What does 'provided to a controller' mean?

The right to object to processing

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right to object to processing

Read the 'At a glance' points and the 'In brief' questions and answers.

You should take some time to read the listed questions but in particular, look at:

- What is the right to object?
- When does the right to object apply?
- Direct marketing
- Processing based upon public task or legitimate interests
- Do we need to tell individuals about the right to object?
- Do we always need to erase personal data to comply with an objection?
- Can we refuse to comply with an objection for other reasons?

Rights related to automated decision making including profiling

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Rights related to automated decision making including profiling

Read the 'At a glance' points and the 'In brief' questions and answers.

At the bottom of the page click on the link to take you to the detailed guidance on special category data. You should take some time to read these paragraphs, but in particular look at:

- What is profiling?
- What is automated decision-making?
- What type of processing is restricted?
- What does 'solely' automated mean?
- What types of decision have a legal or similarly significant effect?
- What are the exceptions?
- What about special categories of personal data?

Find two examples of exceptions where automated decision making, including profiling, is allowed (see the yellow boxes for examples).

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022