The Data Use and Access Act 2025 (DUAA) - summary of the changes to data protection law

▸ Latest updates - 19 June 2025

This summarises the changes the DUAA makes to data protection law that may affect you if you're an organisation using personal information.

It isn't a replacement for our existing guidance for organisations that we will update over time, and as the changes come into effect. It should, however, help you understand what the changes are in the meantime. You can find more details about the updates we're working on in Our plans for new and updated guidance.

This is a factual summary of the changes that each relevant section of the DUAA makes, but it does not cover how you interpret or apply the law. We'll address this as we develop and update our guidance for organisations, in consultation with relevant stakeholders.

It's aimed at data protection experts, including Data Protection Officers (DPOs) and people with specific data protection responsibilities. It's for people who already understand the current law. It explains what has changed rather than providing a comprehensive guide or explanation about data protection law.

If you'd prefer a brief overview of how the DUAA might affect your organisation, please see The Data Use and Access Act 2025 (DUAA) - What does it mean for organisations?.

If you'd prefer a brief overview of how the DUAA affects law enforcement agencies, please see The Data Use and Access Act 2025 (DUAA) - What does it mean for law enforcement agencies?.

If you'd prefer a brief overview of how the DUAA might affect how your own personal information is used by organisations, please see The Data Use and Access Act 2025 (DUAA) - How does this affect me?.

This guidance follows the order and headings in the DUAA for ease of reference. It summarises all the significant changes.

If a section makes minor, consequential, or technical changes that don't significantly change the law, we've noted this without explaining the detail.

If a section makes changes that don't directly affect you, we've noted this without explaining the detail (eg changes to the ICO's responsibilities or the powers of the Secretary of State).

If the DUAA changes the law that applies to competent authorities which use personal information for law enforcement purposes (part 3 of the Data Protection Act 2018 (DPA)), or to the use of personal information by the intelligence services (part 4 of the DPA), we've noted this. Otherwise, the changes relate to the general use of personal information by other organisations.

Data protection

▶ Latest updates - 19 June 2025

Please give us your feedback

Terms used in this chapter

The 2018 Act and the UK GDPR

This is a provision to explain that this part of the DUAA amends the DPA and the UK GDPR.

Definitions in the UK GDPR and the 2018 Act

Meaning of research and statistical purposes

This section inserts text into the UK GDPR to explain what is meant by:

- processing for the purposes of scientific research;
- processing for the purposes of historical research; and
- processing for statistical purposes.

The inserted text draws on the wording of the existing recitals to the UK GDPR.

The section provides that scientific research can include:

- commercial research;
- processing for technological development or demonstration, so far as these activities can reasonably be described as scientific;
- fundamental or applied research, so far as these activities can reasonably be described as scientific; and
- public health research, but only if conducted in the public interest.

It says that historical research can include processing for the purposes of genealogical research.

Finally, it says that processing for statistical purposes means an organisation can process for statistical surveys or to produce statistical results, so long as it:

- aggregates the results it produced (so they no longer amount to personal information); and

- uses neither the personal information that it used, nor the results it produced, to make decisions or support measures about the people whose personal information it has used.

The main effect of this section is to make the interpretative guidance in the recitals legally binding.

There is one difference in that the recitals cite public health research as an example of scientific research. Whereas the DUAA restricts the type of public health research that can fall within the definition to public health research "where the study is conducted in the public interest" only.

Consent to processing for the purposes of scientific research

This section inserts text into the UK GDPR, to allow broad consent to processing for the purposes of scientific research.

It draws on the wording of the existing recitals to the UK GDPR. The effect is to make the interpretative guidance in the recitals legally binding.

It allows people to consent to their personal information being used for an "area of scientific research", so long as:

- it was not possible for an organisation to identify the exact purpose of the research at the time it obtained the consent;
- seeking consent about the area of scientific research is consistent with generally recognised ethical standards relevant to the area of research; and
- people are given the opportunity to only consent to processing for part of the research.

Consent to law enforcement processing

This section inserts the definition of consent already present in the UK GDPR into part 3 of the DPA that applies to law enforcement processing by competent authorities.

Data protection principles

Lawfulness of processing

This section introduces a new lawful basis for processing into the UK GDPR.

The new lawful basis allows processing that is necessary for reasons specified in an annex of "recognised legitimate interests". This annex is inserted into the UK GDPR by schedule 4 - lawfulness of processing: recognised legitimate interests to the DUAA.

It differs from the 'standard' legitimate interests lawful basis for processing. There is still a necessity test, but there is no requirement for an organisation to carry out an additional balancing test to balance the benefits of this processing against the impact on the rights and freedom of the people whose personal information it is using.

This section also amends the 'standard' legitimate interests lawful basis for processing by inserting, and defining, some examples of processing that may be necessary for a legitimate interest. These are:

- direct marketing;
- intra-group transfers for administrative purposes; and
- ensuring the security of network and information systems.

These examples are taken from the recitals to the UK GDPR, so the effect is to make existing interpretative guidance in the recitals legally binding.

This section also adds some wording to clarify that the existing public task basis only applies to the organisation's own tasks. This means an organisation supporting a public authority in the exercise of its tasks should rely on another basis, such as legitimate interests (or the new recognised legitimate interests basis).

It also makes some changes to related powers of the Secretary of State.

The purpose limitation

This section restructures and makes some amendments to the existing provisions that set out when an organisation can consider a new use of personal information to be compatible with the original purpose it collected it for.

It confirms that these provisions apply in addition to, not instead of, the requirement to satisfy a lawful basis for processing.

It provides two slightly different sets of rules. One for personal information that an organisation originally collected under the lawful basis of consent (consented personal information). And one for use when an organisation originally collected the personal information under any of the other lawful bases for processing (non-consented personal information).

For consented personal information the rules are more restrictive and provide that a new use is only considered compatible if an organisation:

- gets consent for the new use;
- carries out the processing to comply with a data protection principle;
- uses the information for a reason listed in a new annex of "processing to be treated as compatible", and it is not reasonable to expect it to obtain new consent; or
- carries out the processing because it is necessary for certain public interest reasons listed in article 23(1) of the UK GDPR, and it is not reasonable to expect it to obtain new consent.

For non-consented personal information this section provides that a new use is considered compatible if an organisation:

- gets consent for the new processing;
- carries out the processing for the purposes of research, archiving in the public interest or statistical processing, and in accordance with the provisions relating to this processing;
- carries out the processing to comply with a data protection principle;
- uses the information for a reason listed in a new annex of "processing to be treated as compatible"; or
- carries out the process because it is necessary for certain public interest reasons laid down by law and listed in article 23(1) of the UK GDPR.

The annex of "processing to be treated as compatible" is inserted into the UK GDPR by schedule 5 - purpose limitation: processing to be treated as compatible with original purpose to the DUAA.

The provisions for non-consented personal information don't say that these are the 'only' circumstances in which new processing can be compatible. Therefore, there also remains the option for an organisation to assess compatibility for this type of processing.

This section confirms the matters that an organisation should take into account when assessing compatibility in this way (also known as applying the compatibility test). These are the same matters as already apply under the pre-DUAA UK GDPR and so we've not listed them here.

It also makes some changes to related powers of the Secretary of State.

Processing in reliance on relevant international law

This section amends the public task lawful basis for processing that applies when an organisation uses personal information for the purposes of:

- carrying out a specific task in the public interest that is laid down by law; or
- exercising an official authority that is laid down by law (eg a public body's tasks, functions, duties or powers).

The amendment provides that relevant international law (as listed in a new schedule) as well as UK domestic law, can provide, or 'lay down', the legal basis for this processing.

The section designates the "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, signed on 3 October 2019" as relevant international law, by adding it to the new schedule. This is an agreement that facilitates the transfer of some telecommunications information between the UK and the US.

It makes a similar amendment to allow relevant international law (as listed in the new schedule) to lay down an article 23(1) public interest reason for the further processing of personal information.

It also authorises the use of special category or criminal offence information based on the same list of relevant international laws.

Processing of special categories of personal data

Elected representatives responding to requests

This section extends the time period in which outgoing MPs, or other elected representatives, can continue to process special category personal information for the purposes of responding to requests from their former constituents. The section extends this period from four days to 30 days after the date of the relevant general election.

Processing of special categories of personal data

This section makes some changes to the powers that the Secretary of State has for the special categories of personal information provisions.

Data subject rights

Fees and reasons for responses to data subjects' requests about law enforcement processing

This section provides that if a competent authority refuses to deal with a request because it considers it to be manifestly unfounded or excessive, then it must:

- tell the person making the request why it has refused it; and
- advise them of their right to complain to the ICO.

It must do this without undue delay and within a set time limit. This mirrors existing requirements on other organisations who are not competent authorities.

It also makes some changes to related powers of the Secretary of State.

Time limits for responding to data subjects' requests

This section provides that the time limit an organisation has to respond to requests from people whose personal information it is using (data subjects) commences when an organisation receives:

- a request;
- further information it has requested and reasonably needs to identify the information or use of information that the request is about; or
- a fee it has requested for a manifestly unfounded or excessive request.

This section also inserts new provisions into parts 3 and 4 of the DPA to allow competent authorities and intelligence services to extend the time they have to comply by up to two months, due to the complexity or number of requests from a particular requester. This aligns with the existing provision in UK GDPR.

Information to be provided to data subjects

This section amends the requirements about an organisation providing people with privacy information.

For article 13 of the UK GDPR (that applies if an organisation collects personal information directly from the person whose information it is using) the section provides that an organisation doesn't have to provide privacy information if:

- it intends to further process personal information for research purposes, in accordance with the provisions covering this type of use; and
- providing the privacy information is impossible or would involve a disproportionate effort.

In these cases, an organisation must protect people's rights in other ways, including by making the information publicly available.

For article 14 (that applies if an organisation obtains personal information from someone other than the person whose information it is using) the section doesn't change the requirements. But it does amend them so they are easier to follow.

The section also clarifies that disproportionate effort depends on, among other things:

- the number of data subjects;
- the age of the personal information; and
- any appropriate safeguards applied to the processing.

This is taken from the existing recitals.

Searches in response to data subjects' requests

This section provides that when dealing with requests from people for their information (subject access requests) an organisation only has to carry out reasonable and proportionate searches for relevant information.

It makes the same amendment to law enforcement and intelligence services processing.

Data subjects' rights to information: legal professional privilege exemption

This section applies to processing by a competent authority for law enforcement purposes. It introduces a new exemption from the right of subject access, for information that is subject to legal professional privilege (LPP).

It provides that if a competent authority decides to claim the exemption, it must inform the person who has made the request about:

- this decision;
- its reasons for making it;
- their right to complain to the ICO; and
- their right to apply to the court to have the decision overturned.

It also provides that these requirements don't apply if providing this information would:

- be subject to LPP itself; or
- conflict with a duty of confidentiality.

The competent authority must maintain a record of its decision not to provide information and give this to the ICO on request.

The section also gives people the right to request that the ICO check that the competent authority has properly applied the exemption.

Automated decision-making

Automated decision-making

This section expands the circumstances in which an organisation can make significant decisions based solely on its automated processing of personal information.

Under the pre-DUAA law, these decisions were restricted unless they were:

- necessary for the purposes of a contract between a person and an organisation;
- permitted by UK law (with appropriate safeguards); or
- done with the consent of the person whose personal information the organisation would use.

This section removes these restrictions, allowing an organisation to make solely automated decisions in a wider range of situations as long as it has appropriate safeguards in place.

The appropriate safeguards are very similar to those that applied under the pre-DUAA law and include that an organisation must:

- provide the person whose personal information it has used with information about the decision;
- enable that person to make representations about the decision;
- enable that person to obtain human intervention about the decision; and
- enable that person to contest the decision.

The effect of this change is to potentially allow an organisation to rely on any of the lawful bases, apart from the new recognised legitimate interests basis, when it makes significant automated decisions about people.

The pre-DUAA law also restricted the use of special categories of personal information in automated decision-making. An organisation could only use this information:

- with consent; or
- where necessary for reasons of substantial public interest, on the basis of UK law that includes suitable safeguards.

This section keeps the restriction on the use of special category personal information.

The section provides that:

- a decision is based solely on automated processing if there is no meaningful human involvement in taking it;
- a decision is a significant decision if it has a legal effect, or a similarly significant effect, on the person whose personal information the organisation is using; and
- when deciding whether there is meaningful human involvement in a decision, an organisation must consider the extent to which the decision is based on profiling.

For law enforcement processing the changes are similar.

The section retains the pre-DUAA restrictions for sensitive processing. These are that a competent authority must:

- base the processing on the explicit consent of the person whose information it is using; or
- be required or authorised by law to make the decision.

It removes these restrictions for non-sensitive processing, so long as a competent authority has appropriate safeguards in place.

The section includes the same safeguards for law enforcement processing as it does for general processing. But it also includes an alternative safeguard of proactive re-consideration of the decision with human involvement.

A competent authority can use this if it is necessary to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or

- protect the rights and freedoms of others.

For law enforcement processing:

- a decision is based solely on automated processing if there is no meaningful human involvement in taking it;
- a decision is a significant decision if it has an adverse legal effect, or similarly significant adverse effect, on the person whose personal information the competent authority is using; and
- when considering whether there is meaningful human involvement in a decision, a competent authority must consider the extent to which the decision is based on profiling.

For intelligence services processing, the DUAA retains the existing restrictions on the circumstances in which an intelligence service can make significant decisions based on entirely automated processing. These are that an intelligence service must:

- carry out the processing because it is necessary for the purposes of a contract with the person whose personal information it is using
- be required or authorised by UK law; or
- base the processing on the consent of the person whose personal information it is using.

This applies for both sensitive and non-sensitive processing.

The DUAA provides that for intelligence services processing a decision is based on entirely automated processing if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision.

Finally, this section also makes some changes to related powers of the Secretary of State.

Obligations of controllers

Data protection by design: children's higher protection matters

This section applies to the providers of online services that are likely to be used by children. They are required to make sure they consider the following when putting in place technical and organisational measures to ensure they comply with the data protection principles:

- How they can best protect and support children using the services.
- The fact that children merit specific protection with regard to their personal information, because they may be less aware of the risks and consequences involved.
- The fact that children have different needs at different ages and at different stages of development.

Logging of law enforcement processing

Logging of law enforcement processing

This section removes the requirement for a competent authority to keep a log of the justification or reasons why it has consulted or disclosed personal information it holds for law enforcement purposes. Other logging requirements remain (such as keeping a log of the identity of the person who has consulted or disclosed the personal information).

Codes of Conduct

General processing and codes of conduct

This section makes some changes to the reporting requirements for bodies charged with monitoring compliance with approved codes of conduct.

Law enforcement processing and codes of conduct

This section makes new provisions that allow the introduction of codes of conduct for law enforcement processing.

It provides that a competent authority may use its adherence to a law enforcement code of conduct to demonstrate its compliance with the law. It also gives an indicative list of topics that a code provider might usefully include in a code of conduct.

Finally, it gives the ICO some related duties, including providing expert bodies with an opinion on draft codes.

International transfers of personal data

Transfers of personal data to third countries and international organisations

This section lists the schedules to the DUAA that make the substantive changes to the international transfers data protection requirements. These are schedule 7 –Transfers of personal data to third countries etc: general processing and schedule 8 - Transfers of personal data to third countries etc: law enforcement processing.

Safeguards for processing for research etc purposes

Safeguards for processing for research etc purposes

This section restructures the provisions about the safeguards that an organisation must apply when processing for the purposes of research, archiving in the public interest and statistical processing. It puts them into a single chapter of the UK GDPR.

There are no substantive changes to the safeguards themselves, although the drafting makes it clear that processing carried out for the purpose of data minimisation, including pseudonymisation, is permitted.

It also makes some related changes to the powers of the Secretary of State.

Section 86: consequential provision

This section makes consequential amendments, as a result of the changes to the research, archiving in the public interest and statistical processing safeguards provisions.

National security

National security exemption

This section introduces a new exemption for law enforcement processing by competent authorities, when this is necessary for the purposes of safeguarding national security.

Although competent authorities are already able to restrict some of the data protection rights that people have if this is necessary to safeguard national security, this provides a wider exemption. It mirrors the national security exemption that already applies to general processing under the UK GDPR.

The new exemption potentially exempts a competent authority from the following requirements:

- The principles, apart from the requirement for the processing to be lawful, and the restrictions and safeguards for sensitive processing.
- The need to comply with people's data protection rights.
- The need to notify people and the ICO about data breaches.
- The provisions about transfers of personal information to third countries, apart from:
  - the requirement that the transfer must be for a law enforcement purpose;
  - the need for the transfer's authorisation, or other justification, when personal information was originally provided by a member state of the European Union; and
  - the rules on subsequent transfers.

The section amends the national security certificate provisions so that they refer to certificates issued under the new exemption, rather than the pre-DUAA provisions.

The section also makes some consequential amendments to other legislation.

Intelligence services

Joint processing for intelligence services and competent authorities

This section introduces new provisions that allow qualifying competent authorities (who are subject to the law enforcement processing provisions in part 3 of the DPA 2018) and intelligence services bodies (who are subject to the intelligence services processing provisions in part 4 of the DPA 2018) to enter into a joint controllership arrangement. So long as the Secretary of State confirms that this is required in order to safeguard national security.

Processing under such an arrangement by a part 3 qualifying competent authority can be designated by the Secretary of State as subject to part 4 intelligence services processing requirements, rather than the usual part 3 requirements.

This would not have been possible under the pre-DUAA provisions and any such joint working would have had to be managed via data sharing agreements and practices.

A competent authority cannot use a designation notice for transfers of personal information outside the UK.

The Secretary of State is bringing forward regulations specifying the qualifying competent authorities that can potentially benefit from these provisions.

Applicants must ensure their request for a designation notice:

- is made jointly by one or more of the qualifying competent authorities, and one or more of the intelligence services;
- describes the processing, including the intended purposes and means of processing; and
- explains why they consider the designation is required for the purposes of safeguarding national security.

Applicants for a designation notice must:

- notify the Secretary of State without delay if they think that the designation is no longer necessary to safeguard national security; and
- provide the Secretary of State, on request, with a description of the processing covered by the notice and an explanation of why they think it is still needed for the purposes of safeguarding national security.

This section sets out what the Secretary of State must do when considering an application and issuing or withdrawing a designation notice.

It also gives the ICO some related duties and provides that a person affected by a designation notice may appeal to the Information Tribunal against the notice.

Joint processing: consequential amendments

This section makes some consequential amendments arising from the introduction of the new joint processing provisions.

Information Commissioner's role

Duties of the Commissioner in carrying out functions

This section makes some changes to the duties of the ICO.

Codes of practice for the processing of personal data

This section inserts a requirement for the ICO to prepare codes of practice, giving guidance about good practice in the use of personal information, if required to do so by regulations made by the Secretary of State.

It says what the ICO must do when it prepares these codes and makes some consequential amendments.

Codes of practice: panels and impact assessments

This section inserts a requirement for the ICO to set up panels to consider codes of practice and sets out the ICO's duties when doing this.

Manifestly unfounded or excessive requests to the Commissioner

This section amends the provisions that allow the ICO to refuse to act on manifestly unfounded or excessive requests, or to charge a reasonable fee for doing so.

The amendments mean that these provisions can apply to any requests, rather than just requests made by people the personal information is about or data protection officers.

Analysis of performance

This section says what the ICO must do when reporting to Parliament annually on how it is carrying out of its functions.

Notices from the Commissioner

This section allows the ICO to serve a notice under the DPA by post and email, rather than only having the option to hand deliver the notice or leave it at the person's usual or last known address.

Enforcement

Power of the Commissioner to require documents

This section makes it clear that the ICO's information notice powers allow it to obtain both information and documents.

Power of the Commissioner to require reports

This section amends the ICO's assessment notice powers, giving it the power to require an organisation to nominate an approved person to prepare a report about a specified matter, and submit that report to the ICO.

The organisation is required to give reasonable assistance to the person preparing the report and to pay their costs.

The ICO is required to either approve the nomination or, if it is not satisfied that the person nominated is suitable, advise the organisation about why it has reached that conclusion and approve a suitable person itself.

If the organisation fails to nominate anyone within the timescale specified in the notice, the ICO is required to approve a suitable person itself.

It gives the ICO the power to issue a fine, if an organisation fails to give the person preparing the report reasonable assistance.

It also gives the ICO a duty to provide guidance on how it exercises these powers.

Assessment notices: removal of OFSTED restriction

This section removes a provision in the pre-DUAA DPA 2018 that exempted OFSTED from the ICO's assessment notices powers.

Interview notices

This section introduces a new power allowing the ICO to compel a person to attend an interview and answer questions, if they work, or have worked, for or on behalf of an organisation that is subject to data protection law. This applies if the ICO suspects that a person or organisation has failed to comply with data protection law or has committed an offence under this law.

Under the pre-DUAA law, an organisation had a general duty to co-operate with the ICO, but the ICO did not have specific powers to make this happen.

It also gives the ICO some related duties and powers and makes some consequential amendments.

Penalty notices

This section extends the time period in which the ICO must issue a penalty notice after the date it issues a notice of intent, from six months to six months or as soon as is reasonably practicable.

It also introduces a new requirement on the ICO to issue a written notice confirming that it is not issuing a penalty notice, if this is the case. It should do so within the same time period, after it issues a notice of intent.

And it requires the ICO to provide guidance on the circumstances in which it would consider it necessary to take longer than six months to issue the penalty notice.

Annual report on regulatory action

This new provision sets out that the ICO must produce and publish an annual report on the regulatory action it has taken. It also specifies what the ICO must include in this report.

Complaints by data subjects

This section introduces a right for people to complain to organisations and competent authorities if they think that they've used their personal information in a way that doesn't comply with the law.

It places an obligation on organisations and competent authorities to help people to make complaints, requiring them to take steps such as providing an electronic complaints form.

They must acknowledge complaints within 30 days and advise the complainant of the outcome without undue delay. They must also take appropriate steps in the meantime, such as making enquiries into the subject matter of the complaint and keeping the complainant informed about progress.

This section also makes some consequential amendments.

Court procedure in connection with subject access requests

This section provides that, if a court orders an organisation to provide it with information (so that it can decide whether or not someone has a right of access to that information) then the court will not be able to order the disclosure of the information, under court procedure rules, until it has made its decision.

It also provides that the court cannot order an organisation to carry out more extensive searches for this information than it would be required to do if the person did have a right of access.

Consequential amendments to the EITSET regulations

This section makes consequential amendments to the ICO's enforcement powers under the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016.

Protection of prohibitions, restrictions and data subject's rights

Protection of prohibitions, restrictions and data subject's rights

This section inserts various amendments to make it clear that provisions about the use of personal information found in other laws, do not override or take precedence over the requirements of data protection legislation. And that nothing within the European Union (Withdrawal) Act 2018 (removal of the principle of supremacy of EU law) changes that.

Miscellaneous

Regulations under the UK GDPR

This section provides that the Secretary of State must consult with the ICO and anyone else they consider appropriate, when exercising their powers to make regulations.

It sets out some limited exceptions to this general rule and specifies some requirements of the Parliamentary negative and affirmative resolution procedures.

Further minor provision about data protection

This section references schedule 11: Further minor provision about data protection that makes some minor and consequential amendments.

Privacy and electronic communications

▸ Latest updates - 19 June 2025

Please give us your feedback

The PEC Regulations

This section explains that the DUAA amends the Privacy and Electronic Communications Regulations 2003 (PECR).

Interpretation of the PEC Regulations

This section amends the definition of a 'call' so that it includes attempts to make a connection via a telephone call, rather than just calls that are actually connected.

It amends the definition of a 'communication' to include information that has been transmitted, rather than just information that has been exchanged or conveyed. This means that texts and emails that have been sent but not necessarily received fall within the scope of the Regulations.

It amends the definition of a 'recipient' of a communication to include an intended recipient.

It inserts the definition of 'direct marketing' that is in the DPA 2018 into PECR. This is "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".

And it clarifies that time periods should be defined in accordance with the Periods of Time Regulation.

Duty to notify the Commissioner of personal data breach: time periods

This section amends the time period within which communications providers need to inform the ICO of a personal data breach from without undue delay or within 24 hours, to "without undue delay and where feasible, not later than 72 hours after having become aware of it".

If an organisation takes longer than 72 hours to advise the ICO about a personal data breach, it must provide the ICO with the reasons for the delay.

This aligns the timeline for notification of PECR security breaches with that of the UK GDPR.

Storing information in the terminal equipment of a subscriber or user

This section amends the rules on storing or accessing information on people's devices or terminal equipment. These are sometimes known as the cookie rules.

It says that storage or access is prohibited unless an exception applies.

The exceptions are listed in schedule 12 - Storing information in the terminal equipment of a subscriber or user that inserts a new schedule into PECR.

It also gives the Secretary of State some powers.

Emergency alerts: interpretation of time periods

This section inserts a minor amendment that clarifies, but doesn't alter, the seven day time limit within which a relevant public communications provider must:

- erase traffic data or location data that it has used to provide an emergency alert service; or
- modify it so that it no longer constitutes personal information.

Use of electronic mail for direct marketing by charities

This section adds a new soft opt-in rule for charities. This allows a charity to send electronic mail marketing, aimed at furthering its charitable purposes, to 'individual subscribers', so long as the charity:

- obtained the email address when the person offered support to, or expressed an interest in, the charity's charitable purposes;
- gave the person the opportunity to opt out of the charity using their details when it first collected them; and
- gives the person the same opportunity each time they contact them.

Commissioner's enforcement powers

This section gives the Secretary of State a power to make regulations to vary the amounts payable under a fixed monetary penalty.

It brings the enforcement powers under PECR into line with UK GDPR, so that enforcement mechanisms and penalties are the same in most cases.

These powers are specified in schedule 13 - Privacy and electronic communications - Commissioner's powers.

Codes of conduct

This section imposes a new duty on the ICO to encourage representative bodies to produce PECR codes of conduct for different sectors and to submit those codes to the ICO in draft.

It sets out what the ICO must do when considering and approving codes and accrediting monitoring bodies.

It sets some requirements for accrediting bodies.

It also provides that an organisation may use its adherence to an approved code of conduct as a means of demonstrating its compliance with PECR.

The Information Commission

▶ Latest updates - 19 June 2025

Please give us your feedback

The Information Commission

This section establishes the Information Commission that replaces the Information Commissioner.

Abolition of the office of Information Commissioner

This section abolishes the office of Information Commissioner that is replaced by the Information Commission.

Transfer of functions to the Information Commission

This section transfers the functions of the Information Commissioner to the Information Commission.

It provides that all references to the Information Commissioner in UK law should be taken to mean the Information Commission.

Transfer of property etc to the Information Commission

This section allows the Secretary of State to set up a scheme to transfer property, rights and liabilities from the Information Commissioner to the Information Commission.

It also allows the Information Commission to continue work started by the Information Commissioner.

Schedules

▶ Latest updates - 19 June 2025

Schedule 4 – Lawfulness of processing recognised legitimate interests

This schedule inserts a new annex into the UK GDPR that sets out the conditions that an organisation needs to meet when relying on the new recognised legitimate interests lawful basis for processing.

These recognised legitimate interests conditions are as follows:

- Disclosures for purposes of processing described in article 6(1)(e):

  This allows an organisation to respond to requests for information from public bodies (or bodies carrying out public tasks) without having to decide whether the requesting body needs the requested information to carry out its public task. Instead, the organisation just needs to make sure the requesting body has confirmed that it needs the information to carry out its public task.
- National security, public security and defence: This allows an organisation to use personal information when this is necessary for the purposes of:
  - safeguarding national security;
  - protecting public security; or
  - defence.
- Emergencies: This allows an organisation to use personal information where this is necessary for the purposes of responding to an 'emergency', as defined by part 2 of the Civil Contingencies Act 2004.
- Crime: This allows an organisation to use personal information where this is necessary for the purposes of:
  - detecting, investigating or preventing crime; or
  - apprehending or prosecuting offenders.
- Safeguarding vulnerable individuals: This allows an organisation to use personal information where this is necessary for the purposes of "safeguarding a vulnerable individual".

This schedule also provides definitions for the "safeguarding vulnerable individuals" recognised public interest condition:

- 'Safeguarding' a vulnerable individual, means:
  - protecting a vulnerable person from neglect or physical, mental or emotional harm; or
    - protecting the physical, mental or emotional well-being of a vulnerable person.
- 'Vulnerable individual' means a person:
  - aged under 18; or
  - aged 18 or over and at risk.
- Protection of a person or of the well-being of a person, includes both protecting a particular person and protecting a type of person.

- A person aged 18 or over is 'at risk' if the organisation has reasonable cause to suspect that the person:
  - has needs for care and support;
  - is experiencing, or at risk of, neglect or physical, mental or emotional harm; and
  - is unable to protect themselves against the neglect, harm or risk, due to those needs.

Schedule 5 – Purpose limitation: processing to be treated as compatible with original purpose

This schedule inserts a new annex into the UK GDPR. The annex provides a list of reuses of personal information that an organisation can assume to be compatible with the purposes for which it originally collected the information, when applying the purpose limitation principle.

Reuse of consented information may be compatible if it's necessary for one of the reasons set out in this annex, but only if it's not reasonable to get consent for that new use.

The list of uses is as follows:

- Disclosures for purposes of processing described in article 6(1)(e): This allows an organisation to respond to requests for information from a public body (or other bodies carrying out public tasks) who have confirmed they need the information for that purpose and to safeguard a public interest objective listed in article 12(1)(c) to (j).
- Disclosure for the purposes of archiving in the public interest: This allows an organisation to make disclosures at the request of an archiving body, provided that:
  - it originally collected the information under the lawful basis of consent;
  - the use of the information complies with the research, archiving, and statistical processing requirements in the UK GDPR;
  - the requesting body confirms that it will only use the information for the purposes of archiving in the public interest; and
  - it reasonably believes that the requesting body will only use the information in accordance with generally recognised standards relevant to its archiving in the public interest.
- Public security: This allows an organisation to use personal information to protect public security.
- Emergencies: This allows an organisation to use personal information to respond to an emergency, as defined by Part 2 of the Civil Contingencies Act 2004.
- Crime: This allows an organisation to use personal information to:
  - detect, investigate or prevent crime; or
  - apprehend or prosecute offenders.
- Protection of vital interests of data subjects and others: This allows an organisation to use personal information to protect the vital interests of the person the personal information is about or another person.
- Safeguarding vulnerable individuals: This allows an organisation to use personal information to safeguard a vulnerable person.
- Taxation: This allows an organisation to use personal information to assess or collect a tax, duty or an imposition of a similar nature.
- Legal obligations: This allows an organisation to use personal information to comply with a legal obligation.

The schedule also provides definitions for the safeguarding vulnerable individuals re-use condition. These are the same definitions as in the new recognised legitimate interests annex inserted by schedule 4 - Lawfulness of processing recognised legitimate interests.

Schedule 6 – Automated decision-making: minor and consequential amendments

This schedule makes minor and consequential amendments to the UK GDPR and the DPA about automated decision-making. These result from the changes to the ADM provisions and include, for example, removing section 14 of the DPA, as this won't be necessary due to the new safeguards in article 22C.

Schedule 7 –Transfers of personal data to third countries etc: general processing

This schedule amends the rules that apply when an organisation transfers personal information to third countries and international organisations.

It amends the description of the standard of protection that is required for these transfers under both adequacy arrangements (now referred to as "transfers approved by regulations"), and alternative transfer mechanisms (now referred to as "transfers subject to appropriate safeguards").

The description of the standard has changed from requiring that "the protection of natural persons guaranteed by the UK GDPR is not undermined", to requiring that the standard of protection provided "is not materially lower" than the standard of the protection provided under the UK GDPR and the DPA 2018. This is now referred to as the data protection test.

The schedule formalises the requirement for an organisation to do a transfer risk assessment for transfers subject to appropriate safeguards. It does this by saying that an organisation must meet the data protection test "reasonably and proportionately".

The schedule also:

- sets out the factors that the Secretary of State must consider when deciding whether the data protection test is satisfied for transfers approved by regulations;
- amends the review period for transfers approved by regulations from four years to "ongoing monitoring"; and
- introduces a new power for the Secretary of State to recognise new transfer mechanisms.

It also makes some other minor changes and restructures some existing requirements.

Schedule 8 – Transfers of personal data to third countries etc: law enforcement processing

This schedule makes the same changes as schedule 7, but for transfers made by competent authorities that use personal information for law enforcement purposes.

It also clarifies that an organisation can make transfers to processors in third countries and international organisations under part 3 law enforcement rules.

Schedule 9 – Transfers of personal data to third countries etc: minor and consequential amendments and transitional provision

This schedule makes minor and consequential amendments about transfers to third countries and international organisations.

Schedule 10 - Complaints: minor and consequential amendments

This schedule makes minor and consequential amendments to the complaints provisions of the UK GDPR and the DPA.

Schedule 11 - Further minor provision about data protection

This schedule makes further minor amendments to the UK GDPR, the DPA and the Victims and Prisoners Act 2024.

These include:

- inserting a definition of direct marketing into the UK GDPR (to match that already used in the DPA);
- providing that time periods are to be defined in accordance with the Periods of Time Regulations; and
- making minor clarifications to some of the special category conditions and exemptions, such as clarifying that:
  - the crime condition and exemption includes the "investigation" of crime;
  - the conditions and exemptions for disclosures for the purposes of journalism and fraud can apply to preparations for disclosure as well as the disclosure itself.

Schedule 12 - Storing information in the terminal equipment of a subscriber or user

This schedule inserts a new schedule into PECR that contains the exceptions from the prohibition on an organisation storing or accessing information on people's devices or terminal equipment (the exemptions to the cookies rules).

The prohibition won't apply if:

- the organisation has provided the subscriber or user with clear and comprehensive information about the purposes, and gives their consent;
- the storage or access is necessary for the sole purpose of carrying out the transmission of a communication over an electronic communications network;
- the storage or access is "strictly necessary" to provide an information society service. (The schedule provides non-exhaustive examples of strictly necessary purposes, including security, fraud prevention, fault detection and authentication);
- the storage or access is for the sole purpose of enabling a service provider to collect information for statistical purposes about how their online service is used;
- the storage or access is for the sole purpose of enabling a service to adapt its appearance or functions in accordance with someone's preferences; and
- the storage or access is for the sole purpose of working out the subscriber or user's geographical location when they request emergency assistance.

Schedule 13 - Privacy and electronic communications: Commissioner's enforcement powers

This schedule amends the ICO's enforcement powers under PECR, to align them with its powers under the UK GDPR and the DPA 18. Most significantly, it:

- removes the requirement to establish that a contravention has caused substantial damage and distress;
- allows the ICO to impose monetary penalties up to a maximum of £17.5m for certain failures to comply;
- replaces the ICO's PECR security audit powers with the power to issue an assessment notice; and
- gives the ICO new powers under PECR, such as the power to compel a witness and the power to commission technical reports.

Schedule 14 - The Information Commission

This schedule:

- makes provisions about the constitution of the Information Commission; and
- includes transitional provisions about the transfer of powers and responsibilities from the Information Commissioner to the Information Commission.