#

# Data Protection

Guidance on the Data Protection Act 2018 and General Data Protection Regulation (GDPR) 2018

# Contents

[About this resource 3](#_Toc11907703)

[Background to data protection law 3](#_Toc11907704)

[The Seven Data Protection Principles 4](#_Toc11907705)

[Fair, lawful and transparent processing 5](#_Toc11907707)

[Collecting and processing personal data 9](#_Toc11907712)

[Storing data 12](#_Toc11907721)

[Data subject rights 14](#_Toc11907728)

[Further resources 15](#_Toc11907731)

# About this resource

The role of Healthwatch requires a significant element of listening to, and recording, people’s experiences of care – whether this information is shared by the person themselves, or by a relative, friend, carer or care professional.

Each local Healthwatch is responsible for ensuring that they comply with data protection laws, including how they record, process, use and store data.

This resource aims to provide you with an understanding to data protection law, and your obligations.

Further guidance can be accessed via the Information Commissioner’s Office

# Background to data protection law

The [Data Protection Act 2018](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) and [General Data Protection Regulation (GDPR)](https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation) have replaced the Data Protection Act 1998. Together they establish a framework to regulate the processing of personal data. This framework balances the legitimate need for organisations and individuals to process personal data with the rights and interests of individuals.

GDPR has strengthened the rights of data subjects and it places additional obligations on data controllers.

The Data Protection Act 2018 contains a limited range of exemptions from parts of GDPR. It also creates GDPR-equivalent measures to areas of data processing that are not covered by GDPR (processing for law enforcement and national security purposes). As such the two pieces of legislation must be considered together.

Data protection legislation applies to **personal data**, information which relates to a living person and from which that person can be identified (from the data itself, or from the data along with other information in the possession of, or available to, the data controller).

**A data controller** is an organisation that makes decisions about the purpose(s) for which, and the way in which personal data is processed. Where a third-party processes data on behalf of a data controller – for example, a contractor hired to send out survey forms – they are a **data processor.** The data controller remains responsible for ensuring that data processors working on their behalf comply with the data protection law.

**Processing of personal data** is a wide term that covers all aspects of obtaining, holding, recording, handling and managing, protecting, altering, consulting, using, sharing, disclosing or disposing of personal data.

Other than domestic purposes (i.e. using personal data for strictly personal and family purposes) that are largely exempt, data protection law (the GDPR and the 2018 Act) applies to and places obligations on anyone who processes personal data. It also creates a number of rights for **data subjects** (people to whom the information relates).

# The Seven Data Protection Principles

Data protection law is underpinned by a set of seven straightforward, common-sense principles known as the Data Protection Principles.

Failure to follow these principles can result in action being taken by the [Information Commissioner's Office](https://ico.org.uk/) (ICO), which can include fines of up to £18 million, however fines will be applied on a proportionate basis.

Data controllers can be sued by data subjects who have suffered loss and/or significant distress due to any breach of the principles.

## The Data Protection Principles:

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’).
2. 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 (‘purpose limitation’).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).
4. 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 (‘accuracy’).
5. 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 (‘storage limitation’).
6. 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 (‘integrity and confidentiality’).
7. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

# Fair, lawful and transparent processing

The first Data Protection Principle requires you to process personal data ‘fairly, lawfully and in a transparent manner’.

Fairness carries its everyday meaning i.e. you must not process personal data in a way that a reasonable person would consider unfair, such as collecting by use of deception or using the data in ways that are unjustified and damaging.

Transparent processing is linked directly to fairness and the right to be informed; it is about ensuring that people have absolute clarity about why they are engaging in an information sharing relationship. This includes where information about a person is collected from a different source – the person detailed has specific rights over their personal data that they need to be able to assert.

## Creating a privacy statement

People who share their data will need to be able to access information on capture, processing, storage and retention or their ‘privacy information’, it is good practice to include this in an organisational privacy statement to which people can be directed to for the information they need.

**Guidance on creating a privacy statement**
We have developed a template to help you create your own privacy statement.

Access the template:

All information needs to be expressed using accessible language and so it can be easily understood by children.

The following privacy information must be supplied to a data subject as a minimum:

* **The name and contact details of the Data Controller.**

A Data Controller is the person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

* **The contact details of the Data Protection Officer (DPO) if you have one.**
* **The purpose for recording, storing and using the personal data. This should include the lawful basis for use.**

Lawful bases are described under Article 6 of the GDPR and any personal data that is collected by an organisation (or other) must be processed for one or more of the 6 reasons described in the Article.

* **Any legitimate interests that may be applicable which detail the benefit derived from processing the data such as the prevention of harm**.
* **The categories of personal data that will be held and used. This includes general data categories as well as special category data.**

General data categories can be the organisation's way of grouping different types of data and helps describe the data type, for example:

* + Employee data
	+ Insight/feedback
	+ Meeting minutes
	+ Contact details

Special category personal data includes:

* + Ethnicity
	+ Political
	+ Religion
	+ Membership
	+ Genetic
	+ Biometric
	+ Health
	+ Sexual orientation
* **The source of the personal data, where it is not collected directly from the data subject**
* **Recipients of the data**Who the recipients of the data will be or the intended audience.
* **Any transfers of the data abroad.**Whether data will be stored on servers or be transferred or processed in any way by countries outside the UK.
* **The amount of time the data will be stored for.**Organisation should have a clear data retention schedule that outlines how long different categories of data will be held for before they are destroyed. This may be a specific time (e.g. “after 3 years”) or criteria for disposal (e.g. “6 months after a case is closed”)
* **The data subject's rights.**This includes the rights of a person to access their data at any time and ask for copies of it. In addition, they must be able to amend their data or have the information they need to make a complaint should they be concerned that their data is not being managed well.
* **The right to complain to the Information Commissioner’s Office (ICO)**
* **Information on the right to withdraw consent and how this can be processed.**
* **How to lodge a complaint.**This should include the details of the Data Controller and who to contact should there be any concerns with the way data is managed or used.

# Lawful processing

For processing to be lawful, personal data must not be processed in a way which breaches any other law, and must also meet at least one specified “lawful basis” for processing under Article 6 of the GDPR.

Under the GDPR the ‘legitimate interests’ condition that could previously be used by public bodies such as local Healthwatch for processing personal data ‘in the performance of their tasks’ (i.e. carrying out your role) is no longer permitted for public bodies in the course of performing their public functions.

Instead there is a new condition that allows processing carried out “in the public interest or in the exercise of official authority vested in the data controller”.

The conditions outlined under Article 6 are:

* **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
* **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
* **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
* **Vital interests:** the processing is necessary to protect someone’s life.
* **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
* **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

## Lawful processing of special category data

Special category data is personal data that relates to: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, or sexual life or orientation. Because this data is more sensitive it requires additional protection.

Information about the commission (or alleged commission) of any offence and proceedings or sentencing for any offence are covered by similar protections under the 2018 Act.

For special category data, organisations will need to identify the lawful basis for processing under Article 6 as well as identifying a condition for processing under Article 9. The Data Protection Act 2018 has introduced additional conditions and safeguards on top of those that are considered in the General Data Protection Regulation.

The lawful basis for processing ‘special category’ personal data are very similar to the last set of conditions that existed under the Data Protection Act 1998. However, the condition relating to ‘medical purposes’ is broadened to cover ‘health and social care purposes’ and there is a separate condition to cover ‘public health’, which is relevant to the service that Healthwatch provides. Article 9 Section 2 (h) is of particular interest to local Healthwatch.

Article 9 (2) of the GDPR outlines the lawful basis for processing special category data:

* **Consent:** the data subject has given explicit consent to the processing of personal data for one or more specified purposes.
* **Legal rights:** processing is necessary in order to meet specific obligations or to exercise specific rights set out in employment law.
* **Vital interests:** processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
* **Certain not-for-profit groups:** processing is carried out by a political, philosophical, religious or trade union group (with some additional conditions). This lawful basis for processing does not apply to the work of Healthwatch.
* **Publicly available:** processing relates to personal data which has been deliberately made public by the data subject
* **Judicial requirement**: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
* **Public interest:** proportionate and appropriate processing is necessary for reasons of substantial public interest, ensuring that certain measures are taken to safeguard the fundamental rights and the interests of the data subject
* **Health and wellbeing:** processing is necessary for the provision of health or social care treatment or services (including preventive or occupational medicine) or the management of health or social care systems and services. This condition only applies where there are legal protections in place to protect the rights of the data subject (e.g. legal requirements of medical confidentiality).
* **Public health:** processing is necessary for reasons of public interest in the area of public health, including ensuring high standards of quality and safety of health care. Measures need to be taken to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
* **Archiving:**  processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

# Collecting and processing personal data

The role of Healthwatch requires a significant element of listening to, and recording, people’s experiences of care – whether this information is shared by the person themselves, or by a relative, friend, carer or care professional. Recording, holding and using this information is the processing of personal and special category personal data.

To comply with the Data Protection Principles, you must ensure that you have a clear understanding of your purpose(s) for obtaining this data and clearly tell data subjects how and why you will use this information.

This can be a fairly broad description – such as ‘carrying out the role of Healthwatch to promote improved care’, but you mustn’t use personal data for purposes that are inconsistent with that description or are likely to come as a surprise to the data subject. Where personal data will be used for more than one purpose, all of the purposes must be explained.

You should also tell people that anonymised data will be shared with Healthwatch England.

If you need to share personal data or confidential personal data, you will need to ensure that you have the data subject’s consent or that you meet another lawful basis to permit this.

For example, where you need to share personal data to assist a local authority to carry out its function to safeguard a vulnerable person from abuse.

Where a person objects to you recording their personal data on any system you must respect their wishes unless you have another lawful basis for the processing *and* a compelling reason to override their wishes.

Where someone shares another person’s personal data with you (e.g. you’re told about someone’s experience of care by a relative) you should consider what reasonable and proportionate steps you can take to make the data subject aware – for example, you could ask the person sharing the information to inform the person who they are sharing information about, or you could consider how else to contact them. As a minimum, you must publish information about how and why you process personal data.

With personal data obtained in this way, you should consider whether you need to record it in identifiable form (would it still meet your needs if the data was anonymised). Where this data is being recorded digitally, you must ensure that you meet necessary conditions for processing personal data and (where applicable) sensitive personal data.

## Data Protection Officers

Local Healthwatch are considered to be public bodies. As such you must appoint a Data Protection Officers (DPO) to monitor and advise on compliance with the data protection law and to liaise with the ICO.

The DPO is a source of expertise for the organisation; they provide advice on how to comply with the GDPR and will be a subject matter expert on data protection. They will also be the ICO’s main point of contact with you. They will liaise directly with senior officers on data protection matters.

The ICO summarises the main elements of their role as follows, a DPO:

* Provides advice to the organisation on compliance obligations and when a data protection impact assessment is required
* Monitors compliance with the GDPR and organisational policies
* Co-operates and liaises with the Information Commissioner
* Considers information risk when performing the above
* Reports directly to the highest management level of the organisation
* Is involved in all data protection issues
* Is supported by the necessary resources and able to maintain expertise
* Will not be pressurised by the organisation as to how to perform his or her tasks, and is protected from disciplinary action when carrying out those tasks
* Has no conflict of interest where they perform other roles

There are several key considerations that Healthwatch must take into account before appointing to this role. The ones that can have significant ramifications for how a DPO can be appointed are listed below:

### The DPO must have no conflict of interest where they perform other roles

The appointed DPO must not be responsible for making decisions about the processing of personal information for the organisation they perform the role for. They are there to monitor and advise.

For Healthwatch this means that anyone with the ultimate responsibility for making decisions about capturing feedback, gaining consent, storing, recording and retaining data cannot be a DPO as there would be a potential conflict of interest.

Given the size of our organisations, it is unlikely that a Healthwatch member of staff with the appropriate level of knowledge and seniority to perform this role would not be involved in organisational decision making about data processing.

It is therefore advised that Healthwatch look to appoint DPOs from external sources, or share DPOs, to avoid non-compliance. If the decision is made to appoint an internal staff member as the DPO then the conflict of interest issue should be addressed clearly.

### The DPO cannot be pressurised by the organisation as to how to perform their task, and is protected from disciplinary action when carrying out those task

Again, this has implications for a smaller organisation. If an internal staff member is appointed, then for the purpose of their DPO role they must sit outside of the management structure – they must have direct access to the most senior managers of the organisation and should not have their activities as DPO restrained by managerial control or sign-off. At the end of the day the DPO may have to report the organisation for a data protection breach and they must be able to do so without interference.

As with the previous requirement it is recommended that due to the size of Healthwatch organisations an internal staff member is not appointed because showing that they are able to work objectively and are not under influence would be extremely difficult to demonstrate.

## Data Protection Impact Assessments

Under the new data protection law where new data processing is being considered, or where changes are planned which may result in a high risk to privacy or data subjects rights, a data protection impact assessment (DPIA) must be conducted to assess and minimise those risks, and privacy protection must be considered from the start and throughout the change.

Data Protection Officers must be included in this process. Where the proposed change carries a high risk to privacy which cannot be adequately mitigated, the ICO must be consulted before the change is actioned.

**Guidance on conducting a Data Protection Impact Assessment**
We have developed a template and guidance to help you create your own Data Protection Impact Assessment.

Find out more: <https://network.healthwatch.co.uk/guidance/2019-02-20/data-processing-impact-assessment-template>

## Consent

Consent is not always required to obtain and process personal data. If lawful bases, as outlined above, are engaged you do not require consent. You should only seek consent if you are prepared to abide by the decision of the person you are collecting information from or data subject.

You should also bear in mind that some people lack capacity to consent. A person with parental responsibility can give consent on behalf of a child who lacks capacity to consent, but no-one can give consent on behalf of an adult. When considering whether an adult is capable of consent, you should assume that they are unless there is evidence to the contrary, and you should consider what support could be given to assist them and support their capacity (e.g. finding a time when they are more capable, communicating in appropriate ways, seeking support from family and carers etc.)

Consent must be specific and informed – the data subject must know what is being asked for and reasonably be able to understand the likely implications. Consent must be given by a positive indication. A nod, a word or a signed form can indicate consent but failure to ‘opt-out’ is ***not*** the same as consent.

The rules on consent have tightened under GDPR. Where consent is being requested, this must be clearly stated and must be separated by other matters. So a request for consent to process data can’t be hidden in the small print or bundled up with other things – each thing you are asking consent for should be set out separately.

Data subjects must be informed of their right to withdraw their consent at any time, and doing so must be as straightforward as giving consent in the first place. Data controllers must maintain evidence to demonstrate that consent has been obtained.

## Recording anonymised information

Where you do not need to record information in a way that identifies individuals, you should record it in anonymised form. Identifiable personal data should only be recorded when there is a clear and lawful reason for doing so.

Where you do not meet necessary lawful bases for processing personal data or special category personal data, or (other than in exceptional circumstances) where the data subject objects to you doing so, you can only process data in anonymised form.

Bear in mind that data is only anonymised where you have not recorded information that would allow you to re-identify it – so a document referring to ‘Mr X’ is only anonymised if you do not hold or have access to other records which reveal Mr X’s identity.

## Data quality

You need to take appropriate steps to ensure that the data you hold and use is accurate and, where necessary, kept up to date. You should retain a record of all of the different data that you store, outlining why it is being kept and for how long. Adding in review dates will mean that you can be prompted to delete data when the retention period has expired. See the section on keeping a log of the data you hold below.

# Storing data

## How long can I keep data for?

You must not keep personal data for longer than is necessary for the purpose(s) for which it was obtained – although that can include a reasonable period of retention necessary for reasons such as audit, dealing with complaints or legal challenge. This means that you must have a sound reason for keeping personal data and once you no longer need it you should securely erase or destroy it.

You should have a retention schedule setting out how long you keep information that you use for various purposes. We have produced a template retention as part of an Information Asset Register for Healthwatch to adapt and use as their own.

**Guidance on creating a retention schedule**
We have developed a template and guidance to help you create your own retention schedule.

Find out more: <https://network.healthwatch.co.uk/guidance/2019-02-05/information-asset-register-guidance-and-template>

## Keeping a log of the data that you hold

Maintaining an Information Asset Register is a robust way to manage information whether it contains personal data or not. It will clearly illustrate data flow within an organisation as well as showing how data is protected and provides an essential source of key information for people who share their data.

Managing a register will also help a Healthwatch comply with data protection requirements while demonstrating that they have good information governance procedures.

An information ‘asset’ is a category of data or type of data set that is routinely collected. So, for example:

* Public experience
* Employment Data
* Annual Reports
* CRM Data
* CRM Data shared with Healthwatch England and so on.

As each asset type has a different set of data contained within it the way you manage that data will need to be evaluated on an individual basis and the register provides a framework for doing this.

Under data protection law Healthwatch must keep ‘records of processing activities’ and must be able to provide those who have entrusted data to them with information, this is outlined in the fair and transparent processing section above.

Other data is also required under data protection regulations and this can be shared through a privacy statement. It is advised that a version of the Information Asset Register should be made available to the public via a link contained within the statement.

**Guidance on creating an Information Asset Register**
We have developed a template and guidance to help you create your own Information Asset Register.

Find out more: <https://network.healthwatch.co.uk/guidance/2019-02-05/information-asset-register-guidance-and-template>

## Keeping data secure

Most fines issued by the ICO are as result of breaches of data security. These include accidental breaches (such as records being left in public places or sent to the wrong people) or as a result of criminal activity, such as hacking, where appropriate security measures have not been put in place.

You must ensure that you have security measures in place that are appropriate to the level of sensitivity of the personal data you store. These measures should include all aspects of processing, including obtaining, holding, using and sharing data. For example, you should ensure that webforms or data collection tools are secure, as well as your main systems and record stores.

Data controllers are required to consider anonymization, pseudonymisation and encryption of data when deciding what security measures are available.

Information security incidents that are likely to place data subjects’ privacy, rights or interests at risk must be reported to the ICO within 72 hours of being identified. Where these incidents carry a high risk to data subjects, those data subjects must also be notified. You will need to have a clear process in place for identifying, escalating and reporting information security breaches.

## Transferring personal data overseas

If you store or process personal data online, in the cloud, or using 3rd party software, you are responsible for ensuring that this data is processed lawfully.

If personal data is processed outside of the European Economic Area (EEA), or the ten other countries assessed as having equivalent levels of data protection, you are required to take additional steps to ensure that the data and subject rights are protected.

In most cases, these rules require some form of additional protection to be put in place, unless the data subject has been made aware of, and specifically consented to the transfer.

If you use systems to store, manage or process data online or in the cloud, you need to check the terms and conditions of the system and ensure that personal data is not being transferred to other countries without the required protection.

The Healthwatch England CRM system holds data in the UK only, and provides secure data storage and mailing systems.

# Data subject rights

### Subject access requests

Data subjects have a right to know what information you hold about them, for what purpose(s), and who you have shared it with.

Where they make a ‘subject access request’ you are required to provide them with a copy of their personal data. Once you have proof of identification you have one month to respond.

You may only charge for responding to subject access requests where the data subject has asked for additional copies of documents, or for manifestly excessive requests. There is a provision to extend the deadline for the most complex requests by a further two months.

There are some exemptions from disclosure – for example, to withhold data of third parties where disclosure would be unfair, e.g. the name of a ‘whistleblower’ who has shared information about a care provider.

You will need a process for managing and responding to subject access requests. The ICO’s website has more information on how to handle these requests.

### Other data subject rights

Data subjects also have further rights, including a right to object to any processing that is likely to cause damage or distress, and the right to ask for inaccurate personal data to be corrected or deleted.

Data subjects have a new ‘right to be forgotten’ – to have data erased where; processing is based on consent, and that consent is withdrawn; the personal data is no longer required; the personal data has been unlawfully processed; or where there are no overriding reasons to continue processing the data.

Where the legal basis for processing for the purpose of tasks carried out in the public interest or in the exercise of official authority (which is likely to apply to much of the data collected by local Healthwatch) people who do not want their data obtained and used will have a right to object. The local Healthwatch would then only be able to obtain and use that person’s personal data where this right is outweighed by ‘compelling legitimate grounds’.

# Further resources

**More information about the Data Protection Act,**

* ICO’s self-assessment toolkit: <https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit/>
* ICO’s guide to data protection:<https://ico.org.uk/for-organisations/guide-to-data-protection/>
* Additional guidance on managing information <https://network.healthwatch.co.uk/resources>
* Advice from Healthwatch England research@healthwatch.co.uk

**More information about GDPR:**

* GDPR guidance from the ICO: <https://ico.org.uk/for-organisations/data-protection-reform/>
* Article 29 Working Party (the group of European data protection regulators – including the ICO) guidance:<http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>
* Information Governance Alliance (which will be publishing GDPR guidance for the health and social care sectors): <https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance>
* Full text of GDPR[: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC](file:///C%3A%5CUsers%5COsmentS%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CRJ3E4VKI%5C%20http%5Ceur-lex.europa.eu%5Clegal-content%5CEN%5CTXT%5C%3Furi%3Duriserv%5COJ.L_.2016.119.01.0001.01.ENG%26toc%3DOJ%5CL%5C2016%5C119%5CTOC) (note: the text starts off with the ‘recitals’ – explanatory notes – before carrying on the Articles of GDPR themselves)
* Data Protection Bill: [https://services.parliament.uk/bills/2017-19/dataprotection.html](https://services.parliament.uk/bills/2017-19/dataprotection.html%20)