

Guide to data processing and protection

January 2023

Contents

Contents	1
About	2
Why complying is important	4
Who is responsible?	7
Policies and processes	10
Collecting data	12
Using data	21
Storing data	23
Data breach	29
People's rights	30
Glossary	32

About

The [Data Protection Act 2018](#) and [General Data Protection Regulation \(UK GDPR\)](#) establish a framework to regulate the processing of personal data. This framework balances the legitimate need for organisations to process personal data with the rights and interests of individuals. In the UK, the Information Commissioner's Office (ICO) ensures that organisations comply with data protection legislation and take enforcement action where the law is broken.

This guidance sets out how Healthwatch can comply with data protection legislation. It covers the following:

- Why you need to comply with the legislation
- Data controllers, processors and data protection officers
- The governance issues that you'll need to take to comply
- How to collect data lawfully
- How to use data lawfully
- How to store data lawfully
- What to do in the event of a data breach
- Data subject rights
- A glossary of data protection terms

This guidance goes beyond explaining the law and describes how to apply it to your work.

The information here is our interpretation of the legislation and regulations. It is not intended and should not be used as legal advice. This document may be subject to change.

The latest version will be available on the Healthwatch Network site for staff and volunteers, and we will issue a notification of any changes.

Whilst Healthwatch England cannot provide legal advice to local Healthwatch, if there are areas of the legislation where you would welcome further clarity, please contact your Regional Manager.

Key points

- Compliance with the law is a must-do for every local Healthwatch. You collect, store and use very sensitive data about people, which could cause them distress if it is revealed. The Information Commissioner's Office could fine you if this happens, which could cause damage to the whole Healthwatch brand.
- You must have a data protection officer in place.
- You need to ensure you have the correct policies and procedures in place and that all your staff and volunteers follow them.
- It's best to rely on another lawful basis other than consent/explicit consent for processing data if possible. We set out possible lawful bases for each type of activity where Healthwatch are processing personal and special category data.
- You must take care when anonymising information about people for publication. It's not just a case of removing names and contact details.
- You must make sure you securely store and manage data.
- You need to have an agreement in place with organisations when you share data with them. You must securely share any data.
- You must take swift action if you have a data breach.
- You must have processes to deal with people's requests to access, correct and stop processing their data.

Why complying is important

Five reasons it's essential to comply with data protection law.

You process a lot of personal data

Healthwatch collect and process Personal data for a variety of purposes:

- As an employer, to recruit people, collect information about your employees, volunteers and Board members
- To carry out your statutory activities, including
 - Listening to, recording and analysing people's experiences of care via engagement or research projects
 - Undertaking research or engagement projects with partners
 - Providing information and signposting to the public
 - Communicating such experiences to third parties through reports
 - Influencing local stakeholders
 - Sharing such experiences with Healthwatch England and, where appropriate, other Healthwatch (e.g. across an ICS area). Please note that Healthwatch England has a data-sharing agreement with Healthwatch that sets out our mutual obligations in protecting and processing such data.
 - Identify and report safeguarding concerns to the local authority and the police.
- To communicate with local stakeholders, you compile lists of your newsletter recipients.
- To find people who might be willing to tell their story as a case study for your website/for use in the media.

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

You are legally required to share data

To carry out your work, you need to share information with others.

For example, it is a legal requirement for Healthwatch to share data with Healthwatch England. Section 221(2)(c) of the Local Government and Public Involvement in Health Act 2007 requires Healthwatch to collect data from people

about their needs for and experience of local health and care services, and Section 221(2)(d)(i) requires you to make those views known to Healthwatch England and (ii) requires you to share your reports with us.

As it is a statutory requirement for you to share data with us, you don't need to ask for people's **Consent** under GDPR, which differs from the everyday and common law meaning of consent. However, we expect you to tell people sharing their experiences with you that you are sharing their data with Healthwatch England.

You must always share the data with us securely.

You collect sensitive personal data

Data protection legislation requires you to have additional safeguards for **Special category data**, including any data about health.

The UK GDPR refers to data 'concerning health' as:

Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.¹

All the data you collect via feedback, signposting, engagement, and research require special consideration, security, and handling. You must have an additional **Lawful basis for collecting special category data**.

Making data anonymous is challenging

Data protection law states that if you cannot identify an individual from the data you hold, referred to as **Anonymisation**, then data protection law does not apply. But if your online survey tool collects any snippet of information that might identify an individual, for example, the IP addresses of those responding, and especially if you have lots of free-text responses, you are likely to be collecting data that could identify people.

Similarly, with qualitative interviews and feedback from engagement, you are likely to be collecting information that could identify individuals. Later in this guide, we explain what issues you'll need to consider if you wholly or partly anonymise data.

You should assume that you will be collecting data that could identify people, including **Special category data** and have procedures to collect, store and use it appropriately. Therefore, you should always take measures to comply with relevant data protection law when undertaking engagement or research activities.

You could damage the Healthwatch brand

The Information Commissioner's Office (ICO) can levy hefty fines and sanctions on organisations that don't comply with data protection legislation. Fines are

¹ Article 4 (15) UK GDPR

usually for data security breaches, including accidental and deliberate breaches or loss of information, such as ransomware attacks or inadequate backups.

However, they can also act when the fundamental rights of individuals are ignored, for example, by not adequately complying with a subject access request. From a regulatory perspective, given the nature of the special category data that Healthwatch processes, the ICO would not accept as a defence that you may be poorly resourced and could, therefore, not protect the information correctly. In 2021, the ICO fined two charities for breaches of data protection legislation - one £10,000 and the other £25,000.

Should you be fined by the ICO for a data breach, it will significantly impact your reputation and the Healthwatch network.

Therefore, you must put in place appropriate technical and organisational measures to store and use data in accordance with the law to minimise the potential of a data breach.

Who is responsible?

What's the role of the data controller, data processor and the data protection officer?

Data controller versus the data processor

The **Data controller**, under the GDPR, now just referred to as the controller, is the organisation or legal entity that decides the purpose(s) of processing and how they will achieve their goal; in other words, what means shall be used. They are responsible for data protection compliance.

Data processor The Data processor will process the data according to the data controller's instructions. They usually help the controller decide 'how' to achieve the purpose of processing.

Your Healthwatch/host organisation is likely to be the data controller. Some Healthwatch contracts stipulate that your local authority is a joint data controller. Other local authorities have decided that they are the data controller and the Healthwatch is the data processor because of how the legislation that set Healthwatch up is worded.

Check your Healthwatch contract or confirm with your local authority. You must name the data controller in your privacy policy. If you need clarification, the ICO has a series of [of handy checklists](#) to help you decide.

When you share data with Healthwatch England, Healthwatch England will become the data controller for the data in their care.

You may use third-party suppliers to assist you in achieving your stated purpose. This could be, for example, a contractor hired to send out survey forms or a survey platform (e.g. SurveyMonkey or SmartSurvey). Or you might be asking a local community organisation to interview people they are in touch with about their experiences of health and care for a report you are writing. Suppliers or contractors who are processing data on behalf of the data controller will be **data processors**.

Your Healthwatch is responsible for ensuring that such data processors comply with the data protection law. This means that you should have performed due diligence on them before sharing any data, and data processing agreements in place regarding how data will be processed and assurances on data security received. You should avoid using processors outside of the UK or EEA.

You must take particular care when sharing data with partners, including other Healthwatch in an ICS area. Before sharing, you must have a robust data-sharing agreement in place and a secure means of securely transferring data. We have provided you with a [template data-sharing agreement](#) to use in these situations. In some cases, you will require consent from the data subject, and you should use precise, unambiguous wording specifically naming the other data controller(s).

Whether or not your host organisation/Healthwatch is a data controller or a processor, your legal entity/Board of Trustees must understand its responsibilities to process data safely and lawfully.

The role of a Data Protection Officer

You must appoint a Data Protection Officer (DPO) as your core activity involves processing large amounts of Special category data.

The role of the DPO is to monitor and advise on compliance with data protection legislation, act as an advocate for the **Data subjects** and liaise with the Information Commissioner's Office (ICO).

Duties of a DPO

The primary duties of a DPO are to:

- Provide advice to the organisation on compliance obligations and when a data protection impact assessment (DPIA) is required
- Monitor compliance with data protection legislation and organisational policies
- Determine if you should report a **Personal data breach** to the ICO and, where necessary, the data subject
- Co-operate and liaise with the Information Commissioner's Office
- Be the contact point for data subjects
- Consider any risks to information when performing the above duties
- Report directly to the highest management level of the organisation
- Be involved in all data protection issues
- In addition, DPOs:
 - Must be supported by the necessary resources and can maintain expertise
 - Cannot be pressurised by the organisation as to how to perform their tasks,
 - Are protected from disciplinary action when carrying out those tasks
 - Must have no conflict of interest where they perform other roles

There are several vital considerations that Healthwatch must consider before appointing to this role. We outline below the issues which affect who can exercise the role of DPO:

Having no conflict of interest

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

For Healthwatch, this means that anyone with 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.

Healthwatch may need to appoint DPOs from external sources or share DPOs, to ensure compliance. If you select an external DPO, someone internally will still need to act as the privacy lead and engage the DPO early when concerns arise. If you appoint an internal staff member as the DPO, you must address the conflict-of-interest issue.

Independent of the organisation when performing tasks

The DPO needs to be independent when performing their tasks. Again, this has implications for a smaller organisation. If you appoint an internal staff member, then for their DPO role, they must sit outside of the management structure. This means 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. The DPO may have to report the organisation for a data protection breach, and they must be able to do so without interference.

Due to the size of Healthwatch organisations, we recommend that you don't appoint an internal staff member because it would be difficult to demonstrate this.

Policies and processes

What you need to do to make sure you have the right governance in place

Key policies

Data protection law requires the data controller to take responsibility for what you do with personal data. You must have appropriate measures and records in place to ensure that you are not only compliant, but you can also demonstrate your compliance. You must have the following measures in place.

Data protection policy

A [data protection policy](#) sets out how you will ensure ongoing compliance with data protection laws. We have provided a template for you to complete.

Privacy statement and cookies policy

A **Privacy Notice**, usually in the form of a privacy policy on your website or a specific data protection statement, outlines how your organisation manages personal information collected as part of any interaction with a member of the public. We have provided a [template for you to complete](#).

A cookie policy on your website sets out how cookies are managed. Cookies are small text files transferred to your computer or mobile when you visit a website or app. These small text files store small pieces of information, usually tracking the user's behaviour on the website. Cookies are a potential privacy risk because they track and store users' behaviour on your website. Therefore, you must regularly update this policy. If you are using the Healthwatch England template website, we have provided a [cookie policy template](#).

Logging information you hold

An **Information Asset Register** sets out the different data 'assets,' i.e. your systems and data repositories (e.g. database), applications (e.g. SmartSurvey) and records that you use for processing personal data. It shows what measures you have put in place to protect the data you are collecting and using.

You should use the Information Asset Register to ensure that crucial processing activities are covered in your privacy notice. You should review it annually as a minimum.

We have provided a [template for an Information Asset Register](#).

Having an information retention schedule

An **Information retention schedule** forms the critical part of your information asset register document. For each type of data you collect, you'll need to specify a time limit for keeping the data.

We have created a template for an [information retention schedule](#) that you can use.

Completing a data protection impact assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

When do I need to carry out a Data Protection Impact Assessment?

You must carry out a DPIA in the planning stages of relevant proposed work. This will enable you to plan privacy protections and mitigate any potential risks to privacy before starting the project.

Is a Data Protection Impact Assessment necessary for every piece of work?

The law does not require you to undertake a DPIA for every processing operation, only for those processing activities that are likely to result in a **high risk** to individuals' fundamental rights and freedoms.

We recommend including these questions in any work planning process and/or project management template.

- Are you collecting any new Personal data or Special category data from people?
- Are you introducing a new database, survey tool or online feedback centre?
- Are you introducing a new data analysis tool?
- Are you working with a new partner to collect data for the first time? For example, are you working with other Healthwatch to collect data across an ICS area?
- Are you engaging a new data processor?
- Are you planning a different approach to collecting and/or storing feedback from the public, e.g. online?
- Would a Personal data breach jeopardise the physical health or safety of individuals?

If the answer to any of these questions is yes, you'll need to write a Data Protection Impact Assessment.

We have provided [a sample template for you](#), which you can adapt to fit your work planning process. If you need help completing one, please contact your Regional Manager.

Collecting data

Applying data protection law when collecting information

You will need to identify the relevant lawful basis for each data type you collect. You must document this in your **Privacy notice**. This is a complex area as it will depend on the purpose or reason you collect data. You can have more than one lawful basis for each activity.

The following sections set out which lawful bases would be appropriate for the key issues where you process personal and special category data. You can find further information about all the lawful bases for processing data on the ICO website [here](#) and special category data [here](#).

Consent and explicit consent

What is consent?

You might think that consent is the best lawful basis to process data as it requires written confirmation that an individual understands how you'll process your data. However, GDPR has a very specific definition of consent:

- **It must be freely given**, meaning that you must give people genuine choice and control and allow them to withdraw consent easily at any time.
- It must be **specific and informed**. It must cover the following:
 - State who the data controller is. This can be in your privacy notice.
 - Explain the purposes of the processing, including separate consent for different processing operations wherever appropriate. This must include all the purposes for which you will use the data. You should include this in the consent form.
 - Outline all the processing activities, including consent options for each type of processing, unless those activities are clearly interdependent. This should be included in the consent form.
 - The right to withdraw consent at any time. Ideally, this should include details of how people can do so. You could cover this in your privacy notice.
- **It must be via an unambiguous indication**. This must be a clear signal that the person agrees. It could include a written statement (in writing or digitally) or orally. It could include ticking a box.

The ICO states that organisations that are in a position of power over individuals should avoid using consent. You might think that Healthwatch doesn't have power over the people it collects data from. However, we have reward and legitimate power due to our statutory powers to promote and support public engagement in the commissioning, provision and scrutiny of health and social care services and

to collect and use local people's experiences of care services to influence the provision of services.

You must keep clear records to demonstrate consent. If someone gives consent over the telephone, you must keep a copy of the script and details of to whom consent was given and when. You should also keep records of what consent wording was in operation at any particular time, for example, historical screenshots of web sign-up pages.

We provide separate guidance on [how to word consent and explicit consent](#).

What is explicit consent?

Explicit consent isn't defined in data protection legislation. The ICO suggests that it must be expressly confirmed in words, separate from any other consents you are seeking. It also states that if you need explicit consent, you should take extra care over the wording. Even when written, not all consent will be explicit. You should always use an express statement of consent. You can obtain explicit consent orally, but you need to keep a record of the script.

What are the alternatives?

- Consent is only one of six lawful bases for processing data, and explicit consent is just one of over 30 lawful bases for processing special category data. We outline below all the possible lawful bases for each type of data collection activity that Healthwatch undertake.
- If you use other lawful bases to process data, you still need to tell people what information you're collecting and how it will be stored, analysed and reported. You'll need to include information about how you'll use any special category data collected. You need to tell people this up front, i.e. at the beginning of a survey or webform to gather feedback or in an information sheet that they are given before an interview or focus group starts. This will allow them to decide whether to participate before you start collecting the data.

Collecting information from the public

Lawful basis for our work

When it comes to collecting personal details and general contact information relating to individuals, there are two lawful bases which you can use:

- Consent²
- It is necessary in the exercise of official authority vested in the controller ("public task")³

If you are collecting data to:

² Article 6(1)(a) UK GDPR

³ Article 6(1)(e) UK GDPR

- Obtain “the views of local people about their needs for, and their experiences of, local care services.”⁴ with a view to making these public or
- Provide “advice and information about access to local care services and about choices that may be made with respect to aspects of those services.”⁵
- Then you will be collecting ‘additional’ sensitive personal information relating to an individual’s health or their health experiences. This additional information falls outside of the scope of GDPR Article 6.

These activities are those that Healthwatch are expected to carry out and are set out in the Local Government and Public Involvement Act 2007. Therefore you can rely on your statutory function as the **Lawful basis** for collecting personal data for processing someone’s data.

You will be collecting data about people’s health and demographics (particularly their ethnicity, health and other data considered ‘special category data’). You’ll therefore need an additional Lawful basis for collecting special category data. There are two possible lawful bases:

- Explicit consent⁶
- Necessary for the provision of health or social care ... or for the management of health or social care systems on the basis of UK law⁷

If you are undertaking an engagement or research project where your anonymised results will be published, you can rely on the research exemption. Therefore, collecting health and other **Special category data** will come under the “substantial public interest.”⁸ lawful basis, as long as the research is considered “scientific”, and there are specific protections under GDPR Article 89(1) and Section 19 of the Data Protection Act 2018.

You must inform individuals what information you are collecting, how you are storing and using it, with whom you are sharing it and for what purpose.

Collecting only the data you need

You’ll also need to ensure that you only collect relevant data that you need for the specific processing activity (Purpose limitation principles). It is best research practice to collect only the information you need for the research project and no more. If, during the initial capture phase, you collected more information than you require for the research work, then the data should be anonymised and minimised wherever possible.

You’ll need to apply this to demographic data collection, too - balancing the need to collect and analyse findings to understand health inequalities with the need to collect only the data that you’ll use.

⁴ Section 221 (2) (c) Local Government and Public Involvement in Health Act 2007

⁵ Section 221 (2) (e) Local Government and Public Involvement in Health Act 2007

⁶ Article 9(2)(a) UK GDPR

⁷ Article 9 (2)(h) UK GDPR

⁸ Article 9(2)(j) UK GDPR

We believe that there is always a case to collect (or ask people) the following demographic questions to consider how different groups will be affected:

- age
- ethnicity
- gender

You'll need to consider whether the issue you are exploring will dictate the need to collect other demographics. For example, if your project is about sexual health services, you will need to collect data about sexual orientation.

We provide guidance on [research planning](#), [survey design](#), a [question bank](#) which includes a wide range of demographics, [collecting demographics](#) and [using demographic data](#) which you may find helpful. Regardless of the processing activity, you should always offer a 'prefer not to say option when collecting special category data. Individuals may also wish to report concerns anonymously, and you should not, therefore, make name and email fields mandatory before submitting a survey form. Please see our separate guidance on [how to word consent and explicit consent](#).

If you need further help with research or engagement design, please contact the Healthwatch Research Team at research@healthwatch.co.uk.

Explaining how you'll use the data

You'll need to provide information to people participating in engagement events and research activities such as interviews, focus groups or surveys to explain the lawful basis and how you'll use their data. If you use cards or forms to obtain public feedback, you'll need to provide this information on paper.

It is best research practice to start a survey/interview with an explanation of the project, what information you are looking for and how you will use the data. Our [guidance on survey design](#) includes a section on what to include in a survey introduction to comply with data protection law.

We have provided template [phone scripts and information sheets](#) for you to use.

When others collect information for you

Some Healthwatch use other organisations to collect data on their behalf - for example, community organisations interviewing their members. In this circumstance, you will need to draw up a data processing agreement with them, setting out the following:

- What data they should collect, and how they should collect it
- How they should store the data
- How they should share the data securely with you

You should also provide them with an information sheet to give to participants explaining that they are collecting the data on your behalf and describing how

you both comply with data protection legislation, and providing links to appropriate privacy notices.

Collecting data about employees and volunteers

Employees and volunteers

In employment matters, including recruitment, the most likely bases for processing standard category (non-sensitive data) will normally be:

- consent⁹
- for the performance of the employee's employment contract¹⁰, or
- necessary in the exercise of official authority vested in the controller¹¹

If you are publishing staff pictures, names, roles and work email addresses or phone numbers on your website, the following lawful bases are appropriate:

- consent¹²
- for the performance of the employee's employment contract¹³.
- Legitimate interest (where Healthwatch are run by Community Interest Companies)¹⁴

Where publication of personal data is a requirement of the role, you must notify staff before they agree to take up employment. If you do this, you must ensure that the requirement is necessary, adequate and not excessive.

The NCVO has helpful guidance on [keeping records on your employees](#).

Your lawful bases for processing personal data on volunteers and board members are the same as for employees.

Special category data - equality, diversity and inclusion

Healthwatch England has set out its vision for itself and the network to tackle health inequalities in the [Equality, Diversity and Inclusion roadmap](#). This includes steps to understand better the diversity across the network at board, staff and volunteer levels.

The lawful bases for collecting this data are:

- Explicit consent¹⁵

⁹ Article 6(1)(a) UK GDPR

¹⁰ Article 6(1)(b) UK GDPR

¹¹ Article 6(1)(e) UK GDPR

¹² Article 6(1)(a) UK GDPR

¹³ Article 6(1)(b) UK GDPR

¹⁴ Article 6(1)(f) UK GDPR

¹⁵ Article 9(2)(a) UK GDPR

- Necessary for the purposes of Healthwatch’s obligations and rights under UK employment, social security and social protection law which applies to the employment of staff/volunteers.¹⁶ If this applies, you must be able to identify the specific legislation or official guidance that you are following (e.g. the Equality Act 2010 or current guidance on an official website)
- necessary for the management of health or social care systems on the basis of UK law and subject to a duty of confidentiality under the rule of law¹⁷

We strongly recommend that you collect this data anonymously without asking for names or positions. If you do so, the GDPR will not apply.

Purpose limitation and employee or volunteer management

You must limit your data collection to what is reasonably necessary to fulfil the purpose. This is likely to include:

- Name and contact details
- DBS checks
- Equality monitoring data
- Disabilities and the reasonable adjustments you need to make
- Training records
- For employees, this will also include:
- Sickness records
- Contact details of next of kin (where appropriate)
- Bank details for payment of salary
- Original application form and references.
- Other personal data to manage employment, such as performance and disciplinary matters.
- Photos for ID cards
- Proof of the right to work in the UK¹⁸

There is a need to record other information, such as vaccination status, when it was required to be fully vaccinated against Covid-19 to visit a care home. This should only be collected and kept while it remains a requirement.

¹⁶ Article 9(2)(b) UK GDPR

¹⁷ Article 9 (2) (h) UK GDPR

¹⁸ See <https://www.gov.uk/view-right-to-work>

Legally collecting data in other circumstances

Photos or videos of people for publicity

The lawful bases for processing data under this activity are:

- consent¹⁹
- necessary for performance of a contract with the data subject²⁰

Remember that people who have given consent have a right to withdraw their consent at any time.

Although a picture may reveal something about the subject (e.g. it may indicate their ethnicity, religion, health condition etc.), it would only be processing of special category personal data if the specific intention of the picture is to record or demonstrate that characteristic.

Where this is the intention, you must obtain the person's **explicit consent** to publish the image for this purpose. After this, the special category personal data within the picture will be considered to have been manifestly made public by the data subject.²¹

If:

- You intend to use the picture to record or demonstrate that characteristic that falls within the scope of special category personal data and;
- If the person cannot give explicit consent,

You should only use the photograph with the approval of a relevant person (e.g. next of kin) and where you can demonstrate that the processing is specifically necessary for exercising your statutory function.²²

If the individual can be recognised, and the photo/video is intended for use in the public domain, you must:

- Explain the purpose of recording/photographing and whether images will be shared and reused
- Keep evidence of who, when, what and how you obtained the consent
- Inform the participant of how long you'll use their image and what will happen to the image when this period ends (e.g. you will delete it). You should tell them that the photo may remain in publication longer than expected and stay in existing publications even if they withdraw consent.

We provide a template [photography consent form](#) you can use.

¹⁹ Article 6 (1) (a) UK GDPR

²⁰ Article 6 (1) (b) UK GDPR

²¹ Article 9 (2) (e) UK GDPR

²² Article 9(2)(h) UK GDPR

Mailing lists for publications and newsletters

The only lawful basis for maintaining mailing lists is consent.²³ You should not be collecting special category data about people for this purpose.

Please note that additional rules apply to electronic marketing²⁴, for example, you must have an 'unsubscribe' section in your newsletter. You must:

- Have systems to ensure that you can amend relevant records accordingly and quickly
- Keep records of consent obtained, e.g. in a database

Case studies for publicity purposes

The lawful bases for processing data for this activity are:

- Consent²⁵
- necessary in the exercise of official authority vested in the controller²⁶

The lawful bases for the processing of special category data for this purpose are:

- Explicit consent²⁷
- necessary for the management of health or social care systems on the basis of UK law and subject to a duty of confidentiality under the rule of law²⁸

People who may lack capacity or need reasonable adjustments

It is essential to remember that some people cannot make decisions themselves. Therefore, they will lack the capacity to understand how you use their data.

If you wish to collect personal data from an adult who may lack the capacity to consent, you should provide additional support and additional information to enable them, as far as possible, to make their own choices about how their data is used.

You should consider whether another appropriate adult can support the person or advise and/or agree that participating in a project is in the person's best interests (consultee). This could be a carer, member of the family or care home staff.

Sometimes adults have the capacity but will need additional support to read information and provide consent when personally identifiable information is being collected, for example, people whose first language isn't English or people with learning disabilities. In these situations, you should provide accessible information sheets and consent forms.

²³ Article 6(1) (a) UK GDPR

²⁴ The Privacy and Electronic Communications Regulations 2003 (PECR)

²⁵ Article 6 (1) (a) UK GDPR

²⁶ Article 6 (1) (e) UK GDPR

²⁷ Article 9 (2) (a) UK GDPR

²⁸ Article 9 (2)(h) UK GDPR

Children

Children need particular consideration when you are collecting and processing their data because they may be less aware of the risks involved.

If you process children's data, you should consider the need to protect them from the outset and design your systems and processes with this in mind.

Compliance with data protection principles and fairness should be central to all your processing of children's data.

You need to have a lawful basis for processing a child's data. This should be the same as for adults. You should avoid using consent if possible. Suppose you are relying on consent as your lawful basis for processing. In that case, when offering an online service directly to a child, in the UK, only children aged 13 or over with sufficient mental capacity can provide their consent. We would still encourage you to ask a parent or guardian to obtain consent. For children under this age, you need to get permission from whoever holds parental responsibility for the child.

You should write clear privacy notices for children so that they can understand what will happen to their personal data and what rights they have. Where possible provide an alternative to a written statement, for example, produce a video.

Children have the same rights as adults over their personal data. These include the rights to access their data, request rectification, object to processing and have their personal data erased.

Using data

How should you use data

You must use the data for the purpose for which it was collected and not for any purpose incompatible with the original purpose unless an exemption exists or you can rely upon another lawful basis, such as using the information for research purposes. If you want to use it for other purposes where the only lawful basis is consent, you'll need to seek permission first from the person.

Anonymisation

We often use quotes from people in reports to illustrate our points in research and engagement projects. It's essential to ensure that individuals cannot be identified from these quotes.

Data protection law does not apply to data rendered anonymous so that the data subject is no longer identifiable.

Identifiability is about whether someone is "identified or identifiable". This isn't just about including someone's name but other information and factors that can distinguish them from someone else.

To render data anonymous, you'll need to ask yourself the following questions:

Does the information identify someone (including indirect identifiers)?

Names, addresses and contact details are not the only things that will identify individuals. Indirect identifiers will also tell us about someone, such as their job title, their place of work or the medical treatment they have received. Remember that photographs or voice recordings can also reveal people's identities.

Any risk of identifying someone from the information must be remote to count as anonymised.

For example, a quote might identify someone if it includes the fact that they are housebound, their age and the name of their GP surgery in their town.

What is the context of the information?

To assess the risk of identification, you'll also have to consider what other information might be available to anyone likely to receive it and which might allow them to identify people.

For example, it might be possible for care home staff to identify a resident from a quote in an enter and view visit report if it includes information about their habits, opinions or concerns. They may also be able to identify someone from the "turn of phrase" used in the quotes.

How do you or any recipient want to use the information?

If you are going to publish the information or it is likely to be widely shared, the risk of identifying someone is a lot higher.

What are the consequences of identifying individuals from the data?

As well as considering the risk of identification, you'll need to think about the consequences for the individuals. You should think about the potential damage if someone were to be identified from the information and be confident that you have ensured that the remoteness of the risk of re-identification is appropriate to the level of harm before using or sharing it.

For example, information about people using a sexual health clinic or people who have experienced domestic abuse is particularly sensitive. You'll need to ensure more robust anonymisation to reduce risk than less sensitive data types. You might want to paraphrase what people say or omit parts of the quote.

You may need to change the demographic descriptors used for specific research participants in final publications to conceal their identity when a rare characteristic of that person plays a central role in the research. For example, you are talking about a medical practitioner who is a single specialist of a particular sort in a hospital/local area). Ensure that what's changed does not affect the research conclusions.

See the section later on Pseudonymisation.

Storing data

How to store data safely and legally

The legislation

Data protection legislation requires you to process your data securely. You must have appropriate security to prevent the personal data you hold from being accidentally or deliberately compromised.

This is something all Healthwatch need to get right as we hold very sensitive data about people's health and wellbeing. If we don't comply, it could impact our reputation, especially for Healthwatch reliant on trust and goodwill.

Storage limitation **and integrity and confidentiality** go beyond how you store or transmit information. Every aspect of your processing of Personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete about why you are processing it; and
- The data remains accessible and usable, i.e., if Personal data is accidentally lost, altered or destroyed, you should be able to recover it and prevent any damage or distress to the individuals concerned.

The practical application

You must ensure that you have security measures 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, and working with partners and IT suppliers that you use.

The most important thing for organisations of all sizes is to ensure that the fundamentals of cyber security are in place to protect their devices, networks and systems. The actions below ensure that basic cyber hygiene controls are in place and functioning correctly. This is important under all circumstances but critical during periods of heightened cyber threat.

An organisation is unlikely to be able to make widespread system changes quickly in response to a change in threat, but organisations should make every effort to implement these actions as a priority.

Physical security

The physical security of the equipment is essential to consider as devices containing personal data could be stolen in a break-in or lost whilst away from the office. You should ensure that you protect personal data on your systems against this type of threat.

You also must ensure that you apply the same level of security to personal data on devices that are used away from the office. Many data breaches arise from the theft or loss of a device (e.g. laptop, mobile phone or USB drive), but you should also consider the security surrounding any data you send by email or post.

Digital security

Check that your digital systems software is up to date. Ensure your users' desktops, laptops, mobile devices, software, business systems and operating system are all patched - updates that address security vulnerabilities, including third-party software such as browsers and office productivity suites. If possible, turn on automatic updates.

Check to ensure that you also patch firmware on your organisation's devices. Sometimes this is implemented in a different way than updating software. See the NCSC's guidance: **Device Security Guidance. You need to ensure that their technical and organisation security measures are robust when processing or storing data with a data processor.**

The [National Cyber Security Centre \(NCSC\)](#) has advice on protecting the infrastructure and, by default, personal data held by organisations.

It's not enough to ensure that you have appropriate technical measures in place. You'll also need to complement your technical measures with appropriate policies, governance and oversight. You must provide suitable training for all employees and volunteers on data protection and keeping personal data safe and secure.

Access to data

It's essential to think about who can access what information. Confidentiality of information is crucial, and you should ask staff to ensure that their passwords are unique to your business systems and are not shared across other non-business systems. Make sure passwords for your systems are strong and unique and that any which are not are changed immediately. See the NCSC's password guidance: [Three Random Words.](#)

Review user accounts and remove any old or unused accounts. If you have [enabled multi-factor authentication](#) (MFA) - or two-factor authentication - check it is properly configured. Make sure it is enabled on systems and user accounts according to your policies. Single sign-on should be utilised wherever possible.

Carefully review any accounts with privileged or administrative access and remove old, unused or unrecognised accounts. Ensure that accounts that have privileged access or other rights are carefully managed and, where possible, use MFA.

Privilege can refer to system administration and access to sensitive resources or information to ensure resources are adequately protected.

You must also have a robust leavers process to ensure access is removed from SaaS (cloud) based systems which can be accessed via any internet browser.

Paper notes of interviews/engagement with the public must be kept in a locked cupboard until typed up and stored securely online. The paper copies should then be shredded and disposed of securely.

Remote working

Volunteers and staff working remotely part or all of the time may be using their own devices to access your systems. You'll need a policy on how to do this safely. The NCSC has some [helpful guidance](#). You should not use private emails for work purposes, particularly for sharing data.

Ensure defences are working

Ensure antivirus software is installed and regularly confirm that it is active on all systems and that signatures are updating correctly.

Check your firewall rules are as expected - specifically, check for temporary rules that may have been left in place beyond their expected lifetime.

The [NCSC's device security guidance](#) can help with the secure configuration of common desktops, laptops and mobile devices.

Backing up your data

If you were to suffer a disaster such as fire, flood or theft, you need to be able to get back up and running as quickly as possible.

You must have systems to [back up your data](#) in case of deliberate or accidental loss or damage.

Confirm that your backups are held securely in an encrypted format and running correctly. Perform test restorations from your backups to ensure that the restoration process is understood and familiar.

Check that there is an [offline copy of your backup](#) - and that it is always recent enough to be helpful if an attack results in data loss or system configuration. However, you should only retain data in backups and archives for a short time.

Check your internet footprint

Check that your external internet-facing footprint records are correct and up to date. This includes which IP addresses your systems use on the internet or which domain names belong to your organisation. Ensure that domain registration data is held securely (check your password on your registry account, for example) and that any delegations are as expected.

Perform an external vulnerability scan of your whole internet footprint and check that everything you need to patch has been patched. Internet-connected services with unpatched security vulnerabilities are an unmanageable risk.

Phishing response

Ensure that staff know how to report [phishing](#) emails. Ensure you have a process to deal with any reported phishing emails.

Ensuring that data cannot be accessed from obsolete devices

Data can be stored on the following devices:

- Mobile phones
- Tablets, laptops and PCs
- Scanners and photocopiers
- Cameras
- Deskphones
- Servers
- Dashcams
- Car communication systems that have been connected to mobile phones via Bluetooth

If you are getting rid of any of these devices, you must ensure that data cannot be retrieved from them. This will mean securely sanitising or destroying the items. See [NCSC's guidance](#) on this topic for further details.

Assessing your compliance

The following are valuable tools for you to gauge your current levels of compliance.

ICO Data protection [self-assessment checklists](#)

The NCSC provides [an online tool](#) to help organisations discover how resilient they are to cyber-attacks and practise their response in a safe environment.

Other considerations

Working with third-party suppliers

Many organisations outsource some or all of their IT requirements to a third party. When doing this, you should be satisfied that they treat your data with at least the same level of security as you would. As a data controller, you are responsible for the data you have collected, even when other companies are dealing with it. You should undertake a due diligence check on potential suppliers

before entering into a contract with a third-party supplier covering the following issues:

- How your data will be stored on their systems
- The security of their systems
- The security of personal information
- Whether the data you supply will be shared with other third parties
- Organisational measures they have taken to ensure data security

You should ensure that you have regular security audits of the systems containing your data, as this may help identify any risks that you need to address. The contracts you have in place with your supplier must be in writing and require them to act only on your instructions and comply with certain obligations of data protection legislation.

If you use a third-party supplier to erase data/dispose of/ recycle your IT equipment, ensure they do it adequately and provide you with a certificate of destruction. You could be held responsible if personal data gathered by you is extracted from your old IT equipment when it is resold.

Location of servers

Storing information (data) on servers (where all cloud software and many online packages keep data) outside the UK is a form of transferring data between countries.

Transfers outside of the UK are referred to as restricted transfers to a third country. And there are two types of third countries, 'insecure' and 'secure' third countries. A secure restricted transfer is one to an organisation within the EEA or to a country which has an adequacy decision²⁹. An insecure restricted transfer is a transfer to other countries such as the USA and India. Transfers to insecure countries should be avoided wherever possible.

Restricted transfers might affect:

- Your database or CRM system
- Survey software, e.g. SurveyMonkey/SmartSurvey
- Qualitative software, e.g. Quirkos
- Cloud-based storage, e.g. OneDrive, Sharepoint, Google Drive
- Instant messaging and video conference calls

Double-check to make sure the storage you use meets all your legal requirements. Specifically, you need to be clear about how you remove data from

²⁹ Countries with data protection legislation comparable with the UK GDPR - see <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/>

the system permanently (hard deletion) and if there are circumstances where the storage company would transfer your data to a third country.

You must give people transparent information about transfers of data between countries. Your privacy notice must include information about where your data is transferred.

You'll need to ensure that your Privacy notice covers storage in online feedback centres and online survey tools. Any tools you use to collect or analyse data must comply with this requirement. You'll need to check the licence that includes a data processing agreement between your Healthwatch and the supplier.

Storing data in data collection or analysis tools

This is relevant if you use online survey tools such as SurveyMonkey or qualitative analysis tools such as Nvivo.

Once you have closed an online survey, analysed and written up the findings, you should download the data and save it in a secure place. Then you should delete the survey and all personal data from the survey tool.

Similarly, once you have analysed the data in the analysis tool and written up the findings, you'll need to delete the data from the tool.

You should also remember to delete any video or audio recordings of research sessions.

Storing data in webforms

If you use your website to gather feedback via a webform, this is likely to contain personal data and special category data. You should regularly download data collected in this way, clear the webform and store the feedback securely elsewhere.

Pseudonymisation

You should have systems to ensure that personal data is kept separately and securely from the feedback you collect. If you use a CRM system, check that it has facilities to pseudonymise data. Pseudonymisation is where clearly identifiable information such as a name and address are removed from a record, and an ID or unique reference number (URN) is used in its place.

You need to remember that data that has undergone pseudonymisation remains personal data and is within the scope of data protection law.

Data breach

Understanding the action you should take.

The action you must take

As soon as you become aware of an actual or potential **Personal data breach**, you should promptly follow your internal policy to address it. If the Data Protection Officer decides that the breach is reportable, they must inform the Information Commissioners Office within 72 hours of becoming aware of the data breach. Please note the 72 hours includes non-working days and bank holidays.

We strongly advise that you start acting within 24 hours.

You must:

- Assess the possible negative consequences for individuals (consider whether they might experience emotional distress, physical or material (financial) damage)
- Unless you assess the breach is unlikely to result in a risk to the rights and freedoms of a natural person, you must inform the ICO within 72 hours after becoming aware of the breach. There is a handy [self-assessment tool](#) on the ICO website to determine whether you need to tell them. [This page](#) on the ICO website has details on reporting a breach. Failure to notify the ICO of a breach when required could result in a hefty fine.
- Address the root cause of the breach so that no further data is lost and, wherever possible, data is retrieved. You should also take action to learn from the data breach to see how you could prevent a recurrence. Any breach should prompt a reminder to staff of the lessons learnt and a review of training practices.
- Tell the individuals concerned if the breach is likely to result in a high risk to their rights and freedoms (there are some [examples on the ICO website](#) which show when this might be necessary). Even if you assess that there isn't a high risk to individuals, the ICO may still require you to tell them.
- Keep a record of all breaches, whether or not you have reported them to the ICO.

The Healthwatch Trademark Licence requires you to notify us of any issues that could damage the brand. Please notify Healthwatch England as soon as you become aware of a data breach or data incident. We can help support you.

People's rights

What if someone wants to access, correct or stop you from processing their data?

Data subjects have a right to know what information you hold about them, for what purpose(s), the lawful basis on which you rely to process their data and with whom you have shared it.

The action you must take

When someone makes a Subject Access Request for details of the data you hold about them via any formal communication channel, including a letter, email, or phone, you must provide them with a copy of their personal data.

Once you have reasonable proof of identification, you should respond as swiftly as possible within one month. Complex requests can be extended by a further two months. **Failure to respond breaches data protection legislation and could impact the Healthwatch trademark licence.**

You may only charge for responding to subject access requests where the data subject has asked for additional copies of documents or where requests are manifestly excessive, but this is a very high threshold to achieve.

Remember that an individual has a right to any information related to them, including data within CRM systems, emails, instant messenger (if you use those channels to hold discussions about them), CCTV, and Voice recordings. You will need to redact or remove any information within the files or recordings related to other third parties.

The right of access to information is not absolute, and some exemptions from disclosure exist. For example, you can decline if it would prejudice an ongoing criminal investigation, withholding data about third parties, where information was given in confidence and where disclosure would be unfair, e.g. the name of a 'whistle-blower' who has shared information about a care provider.

Deleting or withholding any information that a data subject is legally entitled to receive is a criminal offence. You must manage requests and responses carefully - your DPO should oversee them.

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 likely to cause damage or distress and the right to ask for inaccurate personal data to be corrected or deleted.

Data subjects have a 'right to be forgotten' - to have data erased where:

- Processing is based on consent, and that consent is withdrawn;

- processing is based on the controller's legitimate interests or public function and where the information is no longer required;
- 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.

You must have processes to respond to people's requests to delete data.

People have a right to object to processing, but it is a qualified right, meaning there may be legitimate reasons why Healthwatch cannot comply with their request. The primary lawful basis that is likely to apply to much of the data collected and processed by local Healthwatch is to fulfil tasks carried out in the public interest or the exercise of official authority. To achieve this legal obligation, certain personal information must be processed.

People can object to capturing and processing data where the information is unnecessary to fulfil the above tasks.

A decision should be made on a case-by-case basis as to whether you should delete all or some of the personal data held by Healthwatch or whether Healthwatch's 'compelling legitimate grounds outweigh this right. Either way, the data subject should be advised of the decision and action taken.

Glossary

A guide to data protection terms and concepts

Anonymisation

This is the process of editing data, e.g. feedback or interview quotes, so that the data subject is not or is no longer identifiable.

Consent

Data protection legislation aims to give individuals control and choice over what happens to their data. You must therefore ensure that participants' consent is:

- Freely given
- Specific to the purpose, which you'll need to explain to them
- Informed
- An unambiguous indication given by a clear affirmative statement (opt-in).
- Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

Consent doesn't have to be in writing, people can give it verbally, but you must document it (e.g. in the interview transcript).

If consent is the lawful basis for processing, the participant has a right to withdraw that consent at any time. It must be as easy for them to withdraw consent as it is to give it.

Data controller

This is an organisation or legal entity that makes decisions about what data is captured, the purpose(s) for which, and how personal data is processed (the purpose and the means). The data controller can be any formal legal entity and is always accountable for compliance.

Healthwatch needs to be clear about who the data controller is, and your legal entity/Board of Trustees must understand its responsibilities.

Arrangements for data controllers differ between Healthwatch. The data controller could be both your local authority responsible for making arrangements for the provision of Healthwatch and the legal entity of your Healthwatch, which are responsible for day-to-day operational matters, referred to as Joint Controllers. Check your Healthwatch contract or confirm with your local authority.

Data processing

This broad term covers all aspects of obtaining, holding, recording, handling and managing, protecting, altering, consulting, using, viewing, sharing, disclosing or disposing of personal data.

Other than for domestic purposes (i.e. using personal data for strictly personal and family purposes) that are primarily exempt, data protection law (the UK GDPR and the 2018 Act) applies to and places obligations on anyone who processes personal data.

Data processor

This is an organisation or legal entity that assists the data controller in achieving their data processing aspirations. They process personal data on behalf of the controller, usually independently deciding 'how' to achieve the processing goal.

Suppose you don't have any purpose of your own for processing the data and only act on someone else's instructions. In that case, you are likely to be a data processor - even if you make some technical decisions about how you process the data.

Data protection impact assessment (DPIA)

A data protection impact assessment (DPIA) is a privacy-based risk assessment used to identify the risks and legality of any data processing activity. Where you are considering new types of data processing, e.g. sharing data across an ICS area is being considered, or where you are planning changes which may result in a high risk to privacy or data subjects' rights, you must conduct a DPIA to assess and minimise those risks. You must consider privacy protection in the development stage before any processing occurs and throughout the change.

Data Protection Officers must be involved in this process. Where the proposed change carries a high risk to privacy which you cannot adequately mitigate, you must consult the ICO before making the change.

Data Protection Officer

Data protection legislation explicitly requires organisations that process personal data on a large scale or of a highly sensitive nature to appoint a Data Protection Officer (DPO). This means that **all Healthwatch must have one**. Healthwatch England advises local authorities to make this explicit in Healthwatch contract terms.

The DPO is to monitor and advise on compliance with data protection legislation and liaise with the Information Commissioner's Office (ICO) and, where appropriate, data subjects.

You can find out more about the DPO's duties [here](#).

The critical issue is that the appointed DPO must have **no conflict of interest** where they perform other roles. Shared or external DPOs can be engaged.

Data subjects

The data subject is the individual who can be identified from the personal data being processed. Data protection legislation creates several rights for **data subjects**.

One of their fundamental rights is for data subjects to know what information you hold about them, for what purpose(s), and with whom you have shared it.

Explicit consent

'Explicit consent' is not defined in data protection legislation but is usually taken to mean consent which has been explicitly outlined and explained and can be evidenced.

Standard consent is defined and must be freely given, specific, affirmative (i.e. opt-in and not opt-out) and unambiguous, and can be withdrawn at any time. The ICO suggests that explicit consent:

- must be confirmed in a clear statement (whether oral or written) rather than by any other type of affirmative action;
- must specify the nature of the special category data; and
- should be separate from any other consents you are seeking.

Information Asset Register

Under data protection law, Healthwatch must keep accurate 'records of processing activities, in other words, what information you hold, where, its origin, with whom you share it etc. This will inform the information published on your public privacy policy, as you must be able to tell people who have provided data how you'll process their data and when you will destroy it.

Information retention schedule

This is a record of the types of data you hold and how long you intend to hold them. The schedule should be clear about when the retention period starts, for example, one year from capture or seven years after employment ends. You must specify the destruction method. You must include the retention period in your privacy notice.

Personal data

This is information that relates to any person that can be identified (from the data itself or from the data along with other information you or a third party possesses).

In practical terms, this would include the following:

- **Individual's details:** the name of the person (first and last) and, in some cases, their initials, nicknames or the names of friends and family members connected to the individual.

- **Contact details:** email addresses and phone numbers, postcode or address. IP addresses (a unique number that identifies a device connected to the internet) collected by some survey software can also identify people.
- **Unique registration numbers:** NHS number or other unique registration number.
- **Specific details:** for example, someone may be identifiable by the location, date and time they had an operation.
- **Circumstantial information:** for example, the only wheelchair user registered at a GP practice will be identifiable by those details.
- **Contextual information:** The person might be the only person in the care home who likes a specific musician or actor - this can be hard to identify, but be vigilant and only record details when necessary.

It can include photographs, videos, CCTV footage, voice recordings, information held in indexed paper files and electronic data.

The UK GDPR does not apply to deceased individuals, but other legislation, such as the common law duty of confidentiality and other laws, such as Access to Medical Records legislation, survive a person's death.

Lawful basis for collecting personal data

To process standard category personal data, you must have a **lawful basis**. These are set out in Article 6 of the UK GDPR. The ones relevant to Healthwatch activities of gathering views and providing information are:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.³⁰
- **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.³¹ The lawful basis is that Healthwatch are required to collect data from the public “about their needs for, and their experiences of local care services.”³² See [ICO guidance for further details](#).

All Healthwatch will also need a lawful basis under Article 9 of the UK GDPR or Data Protection Act 2018 for special category data. See the section below.

Personal data breach

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper

³⁰ Article 6(1) (a)

³¹ Article 6(1)(e) UK GDPR

³² Section 221 (2)(c) of the Local Government and Public Involvement in Health Act 2007

authorisation; or if the data is made unavailable, and this unavailability has a significant negative effect on individuals.

Principles for processing data

You need to know and understand the legal principles of data protection and what they mean for your organisation. They are as follows:

Lawfulness, fairness and transparency

- Use data legally under a permitted lawful basis
- Use data fairly, being transparent, open and honest with people whose data you hold.
- Only use personal data as individuals would reasonably expect.

For more information on the law, see [the ICO guidance](#).

Purpose limitation

This means you must collect data for a specific purpose.

You should not use the information for another purpose incompatible with the original purpose unless you have a lawful reason or have obtained additional consent.

Data minimisation

This involves collecting the minimum amount of information necessary to achieve the stated purpose.

- See the ICO guidance on [purpose limitation](#) and [data minimisation for more information on the law](#).

Accuracy

- Information captured and processed should be accurate, and where decisions are being made on individuals, it must be kept up to date. This applies to factual personal data and opinions/observations about individuals.
- For more information on the law, see [ICO guidance](#).

Storage limitation and integrity and confidentiality

- Store data securely and confidentially.
- Only retain it for as long as is necessary for the purpose captured.

See the ICO guidance on [storage limitation](#) and [security](#) for more information on the law.

Accountability

You must not only be compliant with the above principles but must be able to demonstrate compliance with them. You must:-

- Take responsibility for what you do with data.

- Have in place appropriate oversight and governance and appoint an independent DPO.
- Have records and policies that show what you're doing with data - you must be compliant and demonstrate compliance.
- Provide appropriate and relevant training in GDPR and cyber-security to keep personal information safe.

For information about the law, see [the ICO guidance](#).

Privacy notice

A privacy notice should inform individuals who you are (details of the data Controller and contact details), what information you are capturing, why, for what purpose, the lawful basis for processing, where you will store it, how you will use it, whether you will share it with any third parties and for how long you will keep it. It should also outline people's data protection rights and provide details of the data controller.

This should be publicly available to let individuals know how you'll use their data before providing it. This should be on your website, and you should refer to it whenever you capture data or conduct engagement or research.

Pseudonymisation

This means the processing of personal data so that the personal data can no longer be attributed to a specific person without the use of additional information. You should store the additional information separately. Appropriate technical and organisational measures should be in place to ensure that no unauthorised individual can reidentify the individual from the pseudonymised datasets.

In the case of Healthwatch, this could be separating data about someone's name and contact details from the data, but in such a way that would allow them to be linked, e.g. by use of a reference number.

Special category data

This is personal data that relates to the following:

- racial or ethnic origin,
- political opinions,
- religious and philosophical beliefs or other beliefs of a similar nature,
- criminal records and activity,
- trade union membership,
- biometric data
- genetic data
- physical or mental health or condition, or

- sexual life or orientation.

Because this data is more sensitive, and based on this information, individuals may experience discrimination, it requires additional protection.

As Healthwatch have a legal obligation to collect data about people's experiences of health and social care services, almost all data we collect will contain special category data about their health. Some types of demographic data (ethnicity, religion and belief and sexual orientation) also come under this category.

Lawful basis for collecting special category data

To process special category data, you must have an **additional lawful basis**. These are set out in Article 9 of the UK GDPR or within Schedule 1 of the Data Protection Act 2018. The ones relevant to Healthwatch are:

- **Consent:** the data subject has given explicit consent to the processing of personal data for one or more specified purposes.³³
- **Legal rights:** the processing is necessary in order to meet specific obligations or to exercise specific rights set out in employment law (for employment purposes only, e.g. to provide reasonable adjustments to disabled people)³⁴
- **Provision or management of health or social care systems or services:** the processing is necessary for the management of health or social care systems on the basis of UK law³⁵ and subject to a duty of confidentiality under the rule of law (i.e. the duty of confidentiality established under English common law and enforceable through the courts).

Subject Access Request

Data subjects can make a subject access request where you are required to provide them with a copy of their personal data. Once you have proof of identification, unless the request is very complicated, you should provide the information within one month.

³³ Article 9 2 (a)

³⁴ Article 9 2 (b)

³⁵ I.e. section 221 Local Government and Public Involvement in Health Act 2007




healthwatch

Healthwatch England
National Customer Service Centre
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4PA

www.healthwatch.co.uk

t: 03000 683 000

e: enquiries@healthwatch.co.uk

 [@HealthwatchE](https://twitter.com/HealthwatchE)

 [Facebook.com/HealthwatchE](https://www.facebook.com/HealthwatchE)