How to Document Your Data Processing

Why do I need to do this?

It is a requirement of the Data Protection Act (2018) and the General Data Protection Regulation (GDPR) that all personal data has a legal basis for being shared. The GDPR requires that this is **documented** under the principle of accountability. This document must be made available to the Information Commissioner's Office (ICO) – the regulator for data protection - on request.

Having a record not only fulfils legal requirements, but also helps with subject access requests – it's easier to source data when you know where it's kept – and the information recorded will also form the basis of your privacy notice.

Step One – what do I have?

a) You should audit what personal data[1] you have and where it is stored. For example, care records are stored in this filing cabinet, employee bank details are stored in the payroll system etc.

The filing cabinet or payroll system in the example above are called **information assets**. You need to keep a record of these assets in an **information asset register (IAR)**. We have provided a template with examples. You **do not** need to record every individual file to complete the IAR.

b) When you know what personal data you have, consider whether it is special category. Mark all information assets which contain special category data. Special category data is:

racial or ethnic origin data	genetic data
political opinions	biometric data (for uniquely identifying someone) e.g. fingerprints
religious or philosophical belief(s)	health data (this includes data used for social care e.g. care plans)
trade union membership	data concerning someone's sex life or sexual orientation

c) When you have finished your audit, you need to risk assess each information asset. Ask yourself what would happen if there was a data breach? Then record how you try to prevent breaches e.g. locked cabinets, passwords, etc.

Our template IAR has examples of what this looks like.

The ICO has also produced a template IAR.

[1] Personal data is any kind of data relating to an individual who can be identified.

Step Two - Where is it from and where does it go?

As social care providers, we receive information from a lot of different places. We also share it with others. This is called processing and this "processing" need to be recorded. Now we have our IAR, we need to think about where our data comes from and where it goes.

As a social care provider, you are a data "controller" under GDPR. This means that you need to document specific information about your processing. You need to include:

a. Your organisation name and contact details, your representative and your data protection officer (if applicable);
b. your reason for the processing;
c. the type of people whose data it is and what kind of data it is, e.g. staff – financial information;
d. the people or organisations you share the data with, e.g. the full name and address of a GP surgery;
e. if the data is transferred outside of the EEA you need to include where it's going and what safety precautions you have in place;
f. where possible, how long you intend to keep the different categories of data;
g. where possible, a general description of the technical and organisational security measures used to protect the data.

Any data you marked as being shared externally in your IAR should be included in your Record of Processing Activities (ROPA). You might have heard this being called information mapping. We have provided a template with examples. This template also includes possible locations you might share data with and the types of data you might share.

All data which is physically transferred – either electronically or in hardcopy - must be added to your ROPA. This could include: Computers, Tablets, Smart Phones, CDs, DVDs, Tapes, Answering Machines, (Digital) Photographs, Letters, Documents, Printouts, Notepads, Diaries etc.

You **do not** have to record information shared through face to face discussions or telephone calls but if notes are made then this information may need to form part of your records.

Exceptions for small organisations:

If you have **fewer than 250 employees**, then you do not have to record all of the personal data which you process. You only need to record processing which

1. is not occasional i.e. you don't need to record a one-off exchange; or
2. is likely to result in a risk to the rights and freedoms of individuals; or
3. contains special category or criminal convictions data.

If you have **250 or more employees**, you need to record all processing activities even if they only happen once or are unexpected.

What to do

a) To process **personal** data, the processing must be necessary, i.e. you could not perform a required activity without using the information. Once you know it is necessary then a legal basis for the processing must be given. There is a table on page 4 with the most common legal bases for social care providers.

b) There are 6 legal bases for processing personal data under GDPR and at least **one** should be recorded on the ROPA. There is guidance on each basis on the Key Definitions page. These are called Article 6 Conditions. No one condition is better than any other.

6(1)(a) Consent	6(1)(b) Contract
6(1)(c) Legal Obligation	6(1)(d) Vital Interests
6(1)(e) Public Task	6(1)(f) Legitimate Interest

c) As we know, some personal data is also considered to be **special category**. For most care providers, most of your special category data will be health and care data. To process special category data, you need to fulfil one of the following conditions (Article 9 conditions) **as well as** one of the conditions above:

9(2)(a) Explicit Consent	9(2)(b) Employment, Social Security, Social Protection Law
9(2)(c) Vital interests when an individual is legally or physically unable to give consent	9(2)(d) Legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
9(2)(e) The personal data has been manifestly made public by the individual	9(2)(f) For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
9(2)(g) Substantial public interest	9(2)(h) The provision of health or social care, treatment or the management of health or social care systems and services or the assessment of the working capacity of an employee
9(2)(i) Public health interests	9(2)(j) For archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes

The most common types of information sharing for social care providers and the legal bases are:

Type of processing	Article 6 Condition	Article 9 Condition
Sharing for direct care or administrative purposes (e.g. waiting list management)	6(1)(c) Legal Obligation – because services registered registered with the Care Quality Commission (CQC) are required to maintain contemporaneous records of care under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17, or the Health and Social Care Act 2012, 251B asserts the duty to share information for direct care purposes. or For **NHS or LA funded** care this can be 6(1)(e) Public Task because it has been commissioned by a public body. or For **Privately Funded** care this can be 6(1)(b) Contract	9(2)(h) the provision of health and social care
For legal reasons (i.e. CQC)	6(1)(c) Legal Obligation	9(2)(j) public interest
Safeguarding	6(1)(e) Public Task	9(2)(b) Employment, Social Security, Social Protection Law
Employment purposes	This will depend on the type of employee data collected. In many instances this will be 6(1)(c) Legal Obligation (e.g. when providing details to HMRC – you need to be able to point to the legislation here) In some instances, this might also be 6(1)(f) Legitimate interests (e.g. NMDS-SC submissions)	If special category data (i.e. sick notes) are processed then the condition would be 9(2)(b) Employment, Social Security, Social Protection Law
Criminal records checks (DBS)	6(1)(c) Legal obligation – you have a legal obligation to do DBS checks – there is guidance on this at https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers	Criminal records data is not considered special category data under GDPR, but Article 10 states that it can only be processed via provision in Member State Law – this is covered in the Data Protection Act 2018, Schedule 1, Part 1, Paragraph 2 – For Health and Social Care purposes 2(2)(b) assessment of the working capacity of the employee.

A note on consent: Consent is very important in health and social care. For common law confidentiality purposes, consent (implied or explicit) is still a valid reason for sharing information. Consent is also a legal basis under GDPR, but the GDPR has stricter rules on consent which may be hard to achieve for social care providers. For the purposes of GDPR we recommend that you look for a different legal basis for processing. This does not mean you should change your current consent practices where these are used for common law or best practice purposes.

The Information Governance Alliance has written detailed guidance on consent under GDPR.

d) Once you have completed the legal basis for processing then complete the rest of the ROPA template – you can use your own if you prefer.

e) One of the columns asks about Data Protection Impact Assessments (DPIA). This is a risk assessment specifically focussed on data protection. You only need to complete a DPIA in specific circumstances. The ICO has a checklist to help you need to complete one. As a minimum, we would recommend it as best practice to complete a DPIA for your care records.

Step Three – Privacy Notices

When you process personal data, you need to tell people what you are doing with their data. For example, when you have a new client, you need to tell them that you might share parts of their care data with other health and care practitioners in order to care. This is called a **transparency notice, privacy notice** or a **privacy statement**. In this you need to set out in clear and easily understood language what you do with people's personal data.

Every person doesn't have to see the full notice, but it does need to be publicly available. For example, it might make more sense to provide a new employee with the part of the privacy notice which talks about their data and then tell them where the full notice can be found rather than provide them with a long document.

Much of the data which should be in the privacy notice is also in the ROPA. This is why you should complete the first two steps before writing your privacy notice.

We have provided a draft, but this will have to be altered based on your organisation. Hopefully, once your ROPA is completed this should not be too complicated. The ICO have detailed guidance on privacy notices.