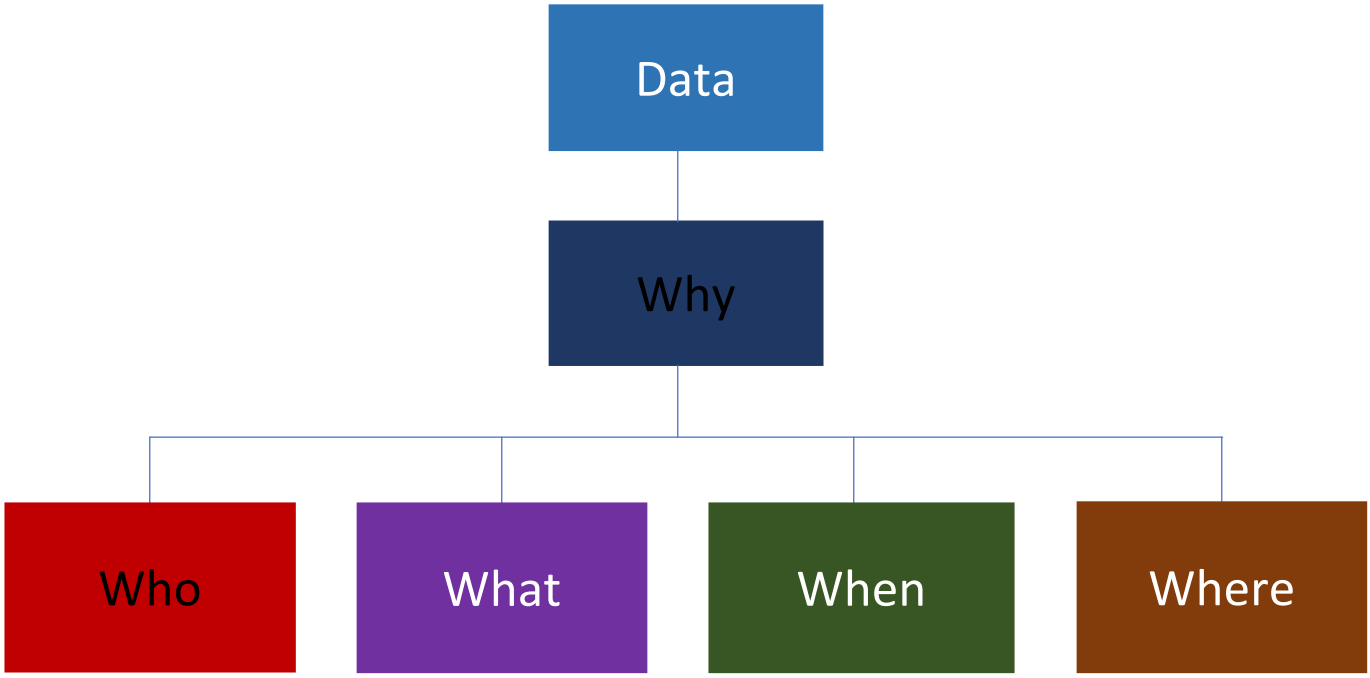
Mapping the 5 W's

This document provides guidance for controllers and/or processors in creating an inventory and map of data processing activities. Think of it as a "how to" manual for the accompanying Data Mapping Record spreadsheet. In many cases, application or contact forms will provide a good point from which to start to follow the data trail for customers or staff.

PLEASE READ ALL INSTRUCTIONS CAREFULLY BEFORE FILLING OUT THIS WORKSHEET



WHY
(Or … What are the REASONS for Processing?)

WHY are Personal Data Processed?

"Personal Data" is broadly defined in the GDPR and means any information relating to a natural person who is *identified or identifiable*. Personal Data includes traditional identifiers like name and address, but also includes IP addresses, application User IDs, GPS data, cookies, biometric data, email addresses, etc. Personal Data includes data that does not, by itself, identify a person, so long as the person is "identifiable" by reference to other available data.

"**Processing**" refers to "*any operation or set of operations which is performed on personal data or on sets of personal data.*" Processing is also broadly defined and includes collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data.

NOTE ON ANONYMIZED DATA: The GDPR does not apply to data that are anonymized in such a way that an individual can no longer be identified from the information on its own, or "reconstituted" with other data to enable identification, as it is no longer "personal data." If you are unsure whether the data are anonymized, assume that data are **not** anonymized.

Consider all areas of the business (not merely backend systems) and list all reasons that Personal Data are used.

Examples of **why** personal data are used include:

- HR and staff administration **– Please note that data that are processed for a company's internal HR are a crucial component of a complete data map**
- Basic client / customer administration
- Legal obligations
- Provision of goods or services
- Marketing and business development activities

WHY are personal data processed?

List the reasons for processing personal data. Please be as clear and concise as possible.

Processing Reason #1:
Processing Reason #2:
Processing Reason #3:
Processing Reason #4:

WHO

WHOSE personal data are processed?

For **each of the reasons** (under "Why are Personal Data Processed?"), list **all of the *categories* of individuals** whose personal data are processed by the Company. Examples of **categories of persons** include:

- Clients (specify duties of individuals at clients:)
- Vendors and business partners
- Healthcare providers (HCPs)
- Grant requestors and other requestors
- Company staff (specify: current/potential/former)
- Relatives/guardians of staff
- Other (describe)

Please ensure that you are as specific as possible in your description of each category. For example, if the general category of persons is "Users," please be more specific. Is it *all* users of the service? If not, which ones?

Complete this page for **each reason** for processing
(from reasons listed under "Why are Personal Data Processed?")

WHOSE personal data are being processed?

Processing Reason #1 (from "Why are Personal Data Processed?"): _____

Processing Reason #2 (from "Why are Personal Data Processed?"): _____

Processing Reason #3 (from "Why are Personal Data Processed?"): _____

Processing Reason #4 (from "Why are Personal Data Processed?"): _____

WHAT

WHAT personal data are processed?

For **each reason** (under "Why are Personal Data Processed?"), list or identify (a) the **type(s) of personal data** collected, received or used, (b) the **source(s) of the data** and (c) the **legal basis** of your collection, receipt or use of the data.

Examples of *types* of personal data:

- Personal details – (specify: name, address, email, telephone, date of birth, emergency contact, sexual orientation, ethnicity, etc.)
- Financial details – (specify: bank account, credit card details, NI, Tax reference etc.)
- Health information
- Images / voice recordings
- 'Know your customer' or due diligence – (specify: passport, tax reference, source of wealth etc.)
- Passport / driver's license / other ID card details
- IP address
- Criminal convictions / offences
- Biometrics – Fingerprint / retinal scan / DNA etc.
- Education and training
- Employment details – (specify: CV, references, annual appraisals, employment status, work permit, leave, sickness, etc.)

***Sources* of the personal data (or … how does the data come into your possession?):**

- Provided by the individual themselves
- Provided by third party individuals authorized by the individuals
- Other sources (specify). Examples:
    - Credit reference agency
    - Criminal record check
    - Internet / social media
    - Government departments / agencies
    - Other public sources (specify)

***Legal basis* (of collection, receipt or use) could be one or more of:**

- Consent – can you provide evidence that consent has been given? Consent must be affirmative, freely given, specific, and informed
- Legal obligation (specify: e.g. – to comply with internal HR requirements)
- Lawful function of public body (specify)
- Protection of vital interests of the individual
- Performance of a contract – may only be used if a *direct* contractual relationship exists
- Legitimate interests of the data controller – ONLY for fraud prevention, network and information security, or facilitating law enforcement

Complete this page (and additional copies if needed) for **each reason** for processing (from reasons listed under "Why are Personal Data Processed?")

WHAT personal data are processed?

Processing Reason #1 (from "Why are Personal Data Processed?"): _____

Type of personal data	Source	Legal basis

Processing Reason #2 (from "Why are Personal Data Processed?"): _____

Type of personal data	Source	Legal basis

WHEN (AND BY WHOM?)

WHEN (and by whom?) are personal data processed?

For **each reason** (under "Why are Personal Data Processed?"), list or identify:

- When were the personal data obtained? (May be on more than one occasion)
- Who within the company accesses (or can access) the personal data?
    - How do these persons access the data?
- Who outside the company has access to or is provided personal data?
    - How do these persons access the data?
- How are the data stored?
- Where are the data stored?
- Are the data updated and kept accurate? How so?
- How long are data retained?
    - How is the retention period determined? (specify – statutory requirement, contract requirement, SOP, etc.)

Complete this page (and additional copies if needed) for **each reason** for processing (from reasons listed under "Why are Personal Data Processed?")

WHEN are the data processed?

Processing Reason #1: _____	
When were the data obtained? (May be on more than one occasion)	
Who has access to the data? … Inside the company? … Outside the company? How are the data accessed by each group?	
Storage: How stored? Where stored?	
Retention: How long are data retained? How is retention period determined?	
Is data updated and kept accurate? How so?	
Processing Reason #2: _____	
When were the data obtained? (May be on more than one occasion)	
Who has access to the data? … Inside the company? … Outside the company? How are the data accessed by each group?	
Storage: How stored? Where stored?	
Retention: How long are data retained? How is retention period determined?	
Is data updated and kept accurate? How so?	

WHERE

WHERE does processing of personal data occur?

For **each of the reasons** (under "Why are Personal Data Processed?"), list or identify where the processing (i.e. access, use, handling, storage, updating, deletion, etc.) occurs.

NOTE: Important to include HR and Admin. Personal Data.

Where **processing occurs (what process, system or service is used and where is the physical location?)**

Examples (may be more than one):

- Manual records – location? (e.g. HR and other admin records?)
- In-house managed systems
- Personal devices (mobile phones, laptops, etc.) / remote working
- External hosted service – (specify: geographic location)
- Cloud service – (specify: geographic location)

Complete this page for **each reason** for processing
(from reasons listed under "Why are Personal Data Processed?")

WHERE does processing of personal data occur?	
Processing Reason #1: _____	
***Where* does processing occur (what process, system or service is used?)** (may be more than one)	
Processing Reason #2: _____	
***Where* does processing occur (what process, system or service is used?)** (may be more than one)	
Processing Reason #3: _____	
***Where* does processing occur (what process, system or service is used?)** (may be more than one)	
Processing Reason #4: _____	
***Where* does processing occur (what process, system or service is used?)** (may be more than one)	