Introduction:

One of the first steps any organisation should take to start on the road towards achieving GDPR compliance, is to carry out a Data Audit. The output of a Data Audit, will be your data inventory, which will show you where all of the personal data you hold, for all different categories of people, is stored and why and how you gathered that data.

Personal data is any information related to a natural person or "Data Subject" that can be used to directly or indirectly identify the person. This information can be anything from their name, date of birth, PPS number, telephone number, location data, fingerprint, medical information, sexual orientation, etc., etc.

The steps below and the accompanying templates can be used as guidance towards the creation of the data inventory. This is a fairly basic method and your organisation may require a more thorough and complex data audit to be carried out on it. There are many applications on the market which would enable more complicated data audits to be carried out, so you may want to look into one of them.

When you carry out this audit, you should involve as many of your staff as possible, because it may turn out that the handling of personal data by front-line staff may be different to the expectation of management. It would be in the best interests of the whole organisation, if the answers provided are honest. This is especially the case where certainty is in doubt. If you don't know the answer to a question, then write "don't know" as the answer. You should endeavour to answer that afterwards.

This data audit technique uses the 5 W's concept: Why, Whose, What, When and Where.

Why?

The following is a non-exhaustive list of examples of why you are processing personal data:

- Client administration
- Direct Marketing
- Provision of goods or services
- Legal obligations
- Employee administration
- Monitoring (e.g. CCTV, web history, Apps, Cookies)
- Profiling of personal data
- Processing for a third party

Whose?

Here you want to list the types/categories of people whose personal data you are processing. Again, this is a non-exhaustive list of examples:

- Clients (specify whether current, former or potential)
- Subscribers
- Business Contacts or Suppliers
- Staff (specify whether current, former or potential)
- Members / Patrons
- Children
- Relatives / Guardians

What?

Here you want to identify the type of personal data that you process, where you sourced it from and what was the legal basis that is in place to process this personal data. Again with the non-exhaustive list of examples:

Types:

- Get specific – Name, Address, e-mail, date of birth, emergency contact, ethnic origin, sexual orientation, etc., etc.
- Financial data – account number, PPS number, credit card details
- Anti-Money Laundering information (photo ID, proof of address, source of funds)
- CCTV, photo or audio recordings
- Biometric information – DNA, retina scan, fingerprint
- Criminal convictions or list of offences
- IP address of computer/mobile device

Source:

- The data subject
- A data controller (sharing with you, as a data processor)
- Social Media platform (e.g. LinkedIn)
- Company Website
- Business card
- Due diligence
- Credit reference check
- Government department

Legal basis:

- Consent (be able to show proof)
- Legitimate interests (specify)
- Performance of a contract
- Legal obligation (specify)
- Lawful undertaking of a public body (specify)

When?

Here you want to show when the data was gathered, who the data was disclosed to and what the retention period is for it.

So for each reason why, you want to show:

- When did you capture or update the personal data
- Have you stated to whom the personal data may be disclosed and under what circumstances
- How long will the personal data be kept and how has this period been determined
  There can be statutory requirements that will govern the data retention period, so be sure to specify which specific regulation is being used to determine this.
  There may be a business-specific practice around data retention. Whatever it is, state it clearly.
  If you believe the retention period should be indefinite, then you will need to have a very strong, clear and lawful reason for such a stance. You may want to consult the Data Protection Commissioner's office to see if it is a justifiable reason.

Where?

Finally, here you want to identify the different places/systems where the personal data is processed.

- What location the paper based records are stored and processed
- Where your digital records are kept (in-house file server, cloud storage (EU or non-EU based), backup disks/tapes, remote/mobile devices)
- What format are the digital records stored in (database. Spreadsheet, document, video file)
- What applications process the personal data (e-mail system, CRM application, etc.) – also whether these are these hosted within the EU or not.