**Data Inventory / Detailed Process Narrative (DI/DPN) Instruction Manual**

The Data Inventory spreadsheet consist of 3 main tabs:

1. ‘**Process 1 DI**’ - Data Inventory - the main tab where all data fields are listed and categorised;
2. ‘**Process 1 DPN**’ - Detailed Process Narrative - the remaining data required for determination of the lawful basis for processing and Article 30 record keeping; and
3. ‘**Metatag**s’ - List of all options for the dropdown lists in ‘Process 1 DI’.

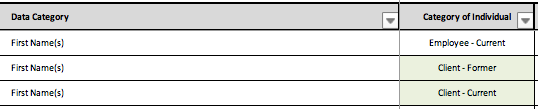
The Data Inventory tab in turn consists of 8 ‘static’ columns, columns titled ‘DATA REPOSITORIES’, and a requirement for a data field applicability indication.

**‘Data Inventory’ Tab:**

Static Columns:

1. ***‘Data Fields’*** - This represents the ‘base unit’ of the entire data inventory / process mapping exercise. Every field used to collect personal data must be listed here.

The examples provided in the template are just that, examples, but should be a good start for most organisations. Any additional data fields specific to your organisation should be added to the bottom of this list. This is for each process owner to determine, and the same Data Field will then be qualified by other ‘Static’ entries, ‘Category of Individual’ for example:



Eventually there will be one large normalised ‘Master List’ of all data fields utilised across your organisation.

*Examples can include: First Name, Last Name, Gender, Mobile Number, Marital Status etc.*

**Action: If your ‘Data Field’ is not listed, add it to the bottom of column A**

1. ‘***Category of Individual***‘ - These are the overarching groups of people that will be used in record keeping and reporting to the supervisory authorities.  
     
   *Examples can include: Employee - Current, Employee - Former, Client - Former, Client - Prospective etc., but these are for you to fully define (see Metatags tab).***Action: If your ‘Category of Individual’ is not listed, add it to the bottom of the corresponding column on the ‘Metatags’ tab.**
2. ‘***Category of Personal Data***’ - Again, these are groups of data that will be used in record keeping and reporting to the supervisory authorities, and provide a summary description of the type of data being processed. While there is no hard-and-fast rule, these descriptions should give some indication as to the risk involved in processing (e.g. ‘Financial Data’ will be more risky than ‘Role Data’).  
     
   *Examples can include: Core Personal Data, National Identity Data, Contact Data etc., but again, these are for you to fully define (see Metatags tab).***Action: If your ‘Category of Individual’ is not listed, add it to the bottom of the corresponding column on the ‘Metatags’ tab.**
3. ‘***Mandatory***’ - This is to give an indication of whether or not the data field is actually *required* for the business process at hand, or just a ‘nice-to-have’. In theory, anything mandatory should be backed up by an existing regulation, a defined legal requirement, or some other documented obligation or business need, but anything that’s nice to have will likely fall more into a requirement for consent[[1]](#footnote-1).  
     
   e.g. Sales may require first name, last name and mobile number for a prospect, but things like gender, nickname, Partner Name are just nice to haves.
4. ‘***Responsibility***’ - For each Data Field are you the ‘Controller’, ‘Processor’, or ‘Joint Processor’.  
    **Note: If you don’t know which you are, just choose [UNKNOWN] from the drop-down list for subsequent review.**
5. ‘***Data Type***’ – This will be one of three things:
   1. **Directly Identifiable Data (DID)** - “*data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain*.” e.g. passport number, SSN/NIN, mobile number etc.
   2. **Indirectly Identifiable Data (IID)**  - “*data that do not identify an individual in isolation but may reveal individual identities if combined with additional data points*.” e.g. even a name is not DID, because there could be many of them (like John Smith), but combine that with Post Code and Age (by themselves IIDs) and you could likely point to a single individual.
   3. **Sensitive Personal Data (SPD)** - any data that relates to the special categories as defined in Article 9(1); “*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*”, or Article 10; “*personal data relating to criminal convictions and offences*”.
6. ‘***Retention***’ – For how long is the data related to this particular business process retained? This retention period should be backed-up by regulatory, legal, or contractual obligation.

**Note: Again, if you don’t know, just choose [UNKNOWN] from the drop-down list for subsequent review.**

1. ‘***Comments***’ - Free-form field for the ‘process owner’s’ notes.

Data Repositories:

This could be one or several dozens of columns wide. However, anything more than about 20 is usually a sign of a process that a) is significantly overcomplicated, b) includes legacy data sources, c) is inadequately defined, and/or d) needs to be further reduced by function.

There are three elements required for data repositories:

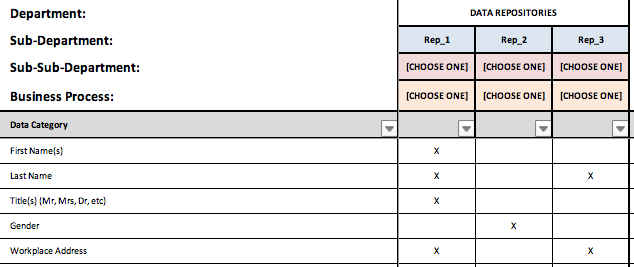
1. ***Name*** - This can be the name of the application, the name of the database, the file source, the name of the hard-copy form and so on. Just looking for ‘friendly’ name at this stage, the name that everyone calls it;
2. ***Functional Responsibility*** – Who manages the data source:
   1. **Internal (EU)** - A department or other business unit that is located within the EU;
   2. **Internal (TC)** - A department or other business unit that is NOT located within the EU
   3. **Third Party (EU)** - A third party provider NOT within your organisation that is located within the EU
   4. **Third Party (TC)** - A third party provider NOT within your organisation that is NOT located within the EU  
        
      **Note: If you don’t know, just choose [UNKNOWN] from the drop-down list for subsequent review.**
3. ***Data Format*** - Whatever medium in which the data is contained and subsequently retained must be recorded. e.g. database, spreadsheet, hard copy etc.  
     
   **Action: If your ‘Data Format’ is not listed, add it to the bottom of the corresponding column on the ‘Metatags’ tab.**

Data Field Applicability Indication:

For every column added to the ‘Data Repositories’ above there will need to be an indication of:

1. ***Is the field use in THIS business process*** - Where the field exists and is actually used in the process an ”X” should be entered.  
     
   **Note: Where the Data Field has absolutely nothing to do with your data source just leave the cells completely blank and these can be filtered out later.**

e.g.



**‘Detailed Process Narrative’ Tab:**

While partially repetitive to the information provided in the Data Inventory tab, the additional information provided in this tab is necessary to provide the legal team the requisite context for their deliberations:

DETAILED PROCESS NARRATIVE

***‘Department’*** - Taken directly from Data Inventory tab;

***‘Sub-Department’*** - Taken directly from Data Inventory tab;

***‘Sub-Sub-Department’*** - Taken directly from Data Inventory tab;

***‘Business Function/Process’*** - Taken directly from Data Inventory tab;

***‘Affected Legal Entities’*** - Should your organisation have multiple legal entities, it’s important to list the relevant ones here. A significant chuck of the action items stemming from this process will involve contractual obligations that must be defined against the appropriate organisational units;

***‘Purpose of Processing’*** - This must tell the reader *exactly* what the process is designed to accomplish. Use as much detail as possible, even if it involves providing samples of the process output, or links to additional documentation.

e.g. “Signing new clients.” is not sufficient, while “Attempting to re-sign former clients using data stored in historical contracts.” Should be in light of all of the other information provided;

***‘Processing Description’*** - Full details of how the process is performed, ideally in the form of step-by-step instructions;

***‘Categories of Individual’*** - List taken directly from Data Inventory tab;

***‘Categories of Personal Data’*** - List taken directly from Data Inventory tab;

***‘External Data Source(s)’*** - For each of the ‘Data Repositories’ on the DI that is an external (third party) source, briefly describe what they are. e.g. data broker. Note: This will not include your clients if you are acting as a processor, this is usually only relevant to you as a controller;

***‘External Data Recipient(s)’*** - To whom do you send personal data? This could be a service provider (e.g. for marketing or loyalty programs), a Government agency (for tax and pension reporting), or even another legal entity within the same enterprise group (e.g. a subsidiary reporting HR matters to ‘corporate’). Note: This will not include sending processed information *back* your clients if you are acting as a processor, this is usually only relevant to you as a controller;

***‘Third Country Transfers’*** - Regardless of whether you are sending personal data to an entity within the same enterprise group, or to a third party, if the personal data is going to a country /region / organisation outside of the EU and not covered under an Article 45 ‘adequacy decision’. You will need to list the ‘organisational and technical security measures’ (or Safeguards) in place to protect the data;

***‘Data Retention’*** – Personal data should only be stored for as long as it required for its purpose. Whether that be a valid business justification, a contractual obligation, or a legal requirement, the time period for storage must be defined and justified;

***‘Security Measures’*** – At a high level, this could be things like; encryption (transit and storage), pseudonymisation, anonymisation, and so on, but behind this is the entire security program documented as ‘technical and organisational security measures’. While it not expected on this form to know the whole extent of the security program in place, security controls at a high level should be general knowledge;

***‘Automated Decision Making’*** – If any of the data processing involved automated decision making (e.g. profiling) this needs to be explained in *full* detail;

***‘Data Location(s)’*** – All locations of the data should be listed here. This may seem repetitive from the above fields, even within the EU national laws may require additional reporting;

FOR [LEGAL TEAM]

The information provided in both the DI and DPN should be enough for the legal team (or external counsel) to make a determination of the:

***‘Lawful Basis for Processing’*** - There should only be one per business process, and it should be only one of the 6 possibilities taken from Article 6;

***‘Rights Available to Data Subjects’*** - Depending on the lawful basis for processing, the data subjects have certain rights. These rights will need to be implemented appropriately. See Annex A for details;

***‘Additional Actions’*** - This is really to entire point of the data/process mapping exercise, the determination of everything required to achieve compliance with the GDPR. Other than determining and implementing the data subject right above, there can be many things left to do.

For example:

1. For every client, a ‘Controller’ Data Protection Agreement (cDPA) should be in place;
2. For every third party involved, a ‘Processor’ (pDPA) should be in place;
3. For data transfers outside the EU, and Data Transfer Agreement (DTA) should be in place that include a description of all security ‘Safeguards’;
4. For each use of legitimate interest (Art. 6(1)(f)), a Legitimate Interest Assessment (LIA) should be performed;
5. For each use of ‘soft consent’, you must ensure that all correspondence has an opt-out feature and a suppression list;

…and so on;

The information in the DI/DPN should be enough for any qualified data protection expert to provide a definitive list of every action item necessary to achieve compliance. If not, it’s their job to tell YOU what’s missing.

***‘Risks / Caveats’*** – There will always be some organisation-specific detail that will leave some form of residual risk, so it’s up to the expert(s) to list any caveats here along with the risks involved.

**‘Metatags’ Tab:**

The Metatags tab is where you list all of the options available to the ‘Data Inventory’ tab. The list provided here are just examples, other than the ‘Responsibility’ column, you can change everything in here to suit your business.

**‘Article 30’ Tab:**

Regardless of what you choose as your DI ‘Data Fields’, you will need to assign each of them to a ‘Category of Personal Data’. The Article 30 tab provides an example of what this might look like for the Data Fields listed on the ‘Data Inventory’ tab.

**‘Article 6’ Tab:**

Over the course of time, each of your business processes will start to fall into pre-defined scenarios that have already been addressed by the experts. This is just a place to keep them for reference (examples provided).

**Annex A - Data Subject Rights According to the Legal Basis for the Processing[[2]](#footnote-2)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rights of the data subject**    **Legal Basis** | **Art. 7 (3)**  Right to withdraw consent | **Art. 13**  Information where personal data are collected from the data subject | **Art. 14**  Information where personal data have not been obtained from the data subject | **Art. 15**  Right to access and right to obtain a copy | **Art. 16**  Right to rectification of inaccurate personal data | **Art. 17**  Right to erasure | **Art. 18**  Right to restriction of processing | **Art. 20**  Right to data portability | **Art. 21**  Right to object |
| **Consent**  Art. 6 (1) (a)  Art. 9 (2) (a) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ |
| **Contract**  Art. 6 (1) (b) | ✘ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ |
| **Legal Obligation**  Art. 6 (1) (c) | ✘ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ | ✘ |
| **Protection of a Vital Interest**  Art. 6 (1) (d) | ✘ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ | ✘ |
| **Public Interest**  Art. 6 (1) (e) | ✘ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ | ✓ |
| **Legitimate Interests**  Art. 6 (1) (f) | ✘ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ | ✓ |
| **Triggered by employment, social security and social protection law**  Art. 9 (2) (b) | ✘ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✘ | ✘ |

1. Please take this opportunity to re-examine the data being processed, is it really necessary? [↑](#footnote-ref-1)
2. There may significant caveats to this, always check with a qualified source. [↑](#footnote-ref-2)