# Data Protection Design plan

See also: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>

## Principles

### Article 25(1)

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

### Article 25(2)

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

## Step 1 – Identify personal data processing

Based upon the activities/processes of your system you want to identify the personal data processing (including recording)

|  |  |
| --- | --- |
| Purpose/Process | Personal data processed |
| Used to reference queries created by the user using the financial analysis API | user\_id |
| Used to authenticate the user with the authentication system | Username and password |

## Step 2 – Link processing purposes

Where multiple processes use the same personal data, link these purposes

|  |  |
| --- | --- |
| Linked purposes | Linked Data |
| Linked with the user queries in the financial analysis API that are used to query other systems for financial information | user\_id in cookie linked with user\_id in API database connected to the quires the user has created |
| Linked to the user account in the authentication system the username and password is used to log into | Username and password to users account |

## Step 3 – Grounds of processing

For each purpose of processing, determine the grounds upon which it is processed.

|  |  |
| --- | --- |
| Processing purpose | Ground of processing (art 6) |
| User\_id is saved in API database and cookie | Consent – The user consents to their id being saved in the API when choosing to contribute to the database whilst logged into a session on their user account. They also consent to a cookie temporarily storing the id once they give the username and password to authenticate themselves and start a session. |
| Username and password are processed | Consent – Information is given freely by the user |

## Step 4 – Data minimalisation

For each processing element, determine whether this is the minimal necessary processing (taking into account the linked purposes)

|  |  |
| --- | --- |
| Processing purpose | Reasons this is minimal |
| User\_id is saved in API database and cookie | Minimal amount of information needed to identify that a query belongs to a user’s account |
| Username and password are processed | This is the bare minimum amount of data needed to log into a user’s account |

## Step 5 – Data deletion/anonymisation

For each processing element/purpose determine how/when this will be deleted or anonymised

|  |  |
| --- | --- |
| Personal data | Deletion/anonymisation process (if applicable) |
| user\_id | User has control over weather the system stores the data as any query containing the user id can be deleted by the user. The user\_id is also deleted once the cookie expires. |
| Username and password | Data is anonymised on input (input is hidden as \*’s and only temporarily kept in memory until the user is authenticated |

## Step 6 – Who processes the data

For each processing element/purpose, determine who will have access to the data

|  |  |
| --- | --- |
| Personal data | Who processes the data |
| user\_id | Not even a user whose data is stored in the API’s database will view their user\_id when returning any information connected with the user\_id (e.g. all the users stored queries) The user\_id is used to retrieved information stored in the financial analysis system API |
| Username and password | Data is sent to the financial analysis API before being passed to the authentication API for authentication |

## Step 7 – Data security

For each processing element/purpose, determine how you will keep this secure (and what is the appropriate security level). This include ensuring that valid users can only access it for the intended purposes

|  |  |
| --- | --- |
| Personal data | Security measures |
| user\_id | This information can’t be returned by any route in the API and is locally stored in the API and in the cookie on the client’s front end. |
| Username and password | Data is anonymised on input and is not stored on any of the systems implemented |

## Step 8 – Informing data subjects

All data subjects must be informed of the processing of their data

|  |  |
| --- | --- |
| Personal data | How/where are subjects informed |
| user\_id | Subjects should be informed that when creating an account the system has the consent to store and process information related to this account |
| Username and password | Users are aware that authenticating themselves requires them to divulge this information to the Web app and API |

## Step 9 – Exercise of rights

How are you going to allow data subjects to exercise their (GDPR) rights: objection, correction, transfer, etc.

|  |  |
| --- | --- |
| Personal data | How/were can subjects exercise their rights |
| user\_id | Users can manage the data via deletion and manual replacement |
| Username and password | Subjects can exercise their rights on this peace of data via the account management system |

# Financial Data Protection Design plan

This system deals with the processing of financial data that is stored by the company for transactions between client and customer such as stock expenditure and order payment. Due to this it is important to understand the sensitivity of the data and handle it appropriately with regard not only to data protection regulations but also to regulations are financial information.

**Personal data protection**

Laws that apply to financial information through it’s usage of personal data. Due to the complexity of these laws especially by proxy no data that can be considered “personal” is stored in the financial information e.g. the data we pull through the orders management system doesn’t contain personal information.

**Anti-laundering fraud**

Financial institutions and businesses handling financial information must comply with **AML** and **KYC** regulations to prevent financial crimes such as money laundering and fraud. This means that any financial data extracted from external API’s should not be modified in any way even if only temporary and/or visually as it can still be utilized to commit fraud.

## Step 1 – Identify financial data processing

Based upon the activities/processes of your system you want to identify the financial data processing (including recording)

|  |  |
| --- | --- |
| Purpose/Process | Financial data processed |
| Information extracted from the API and temporary stored in the financial analysis system’s API and web page when requested | Orders information from order management API |

## Step 2 – Link processing purposes

Where multiple processes use the same financial data, link these purposes

|  |  |
| --- | --- |
| Linked purposes | Linked Data |
| Linked with the user queries in the financial analysis API that are used to provide parameters for the data to be returned from the API | Linked to users’ queries |

## Step 3 – Who processes the data

For each processing element/purpose, determine who will have access to the data

|  |  |
| --- | --- |
| Financial data | Who processes the data |
| Orders information from order management API | This information will be stored on a local database inside the order management system. It can be access through the financial analysis API by an authenticated user. |

## Step 4 – Data security

For each processing element/purpose, determine how you will keep this secure (and what is the appropriate security level). This include ensuring that valid users can only access it for the intended purposes

|  |  |
| --- | --- |
| Financial data | Security measures |
| Orders information from order management API | To get the data through the financial analysis API the user must be authenticated with the right permissions and have the security key for the API |