OneTrust
Privacy Management Software

The Ultimate Data Mapping and GDPR Article 30 Handbook

Everything you need to know to understand, develop, implement, and roll out a GDPR compliant and operationally efficient data inventory and mapping process for your privacy program.

March 21, 2017

Disclaimer
No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

CONTENTS OF THIS HANDBOOK

Part 1: Understand Requirements and Terminology

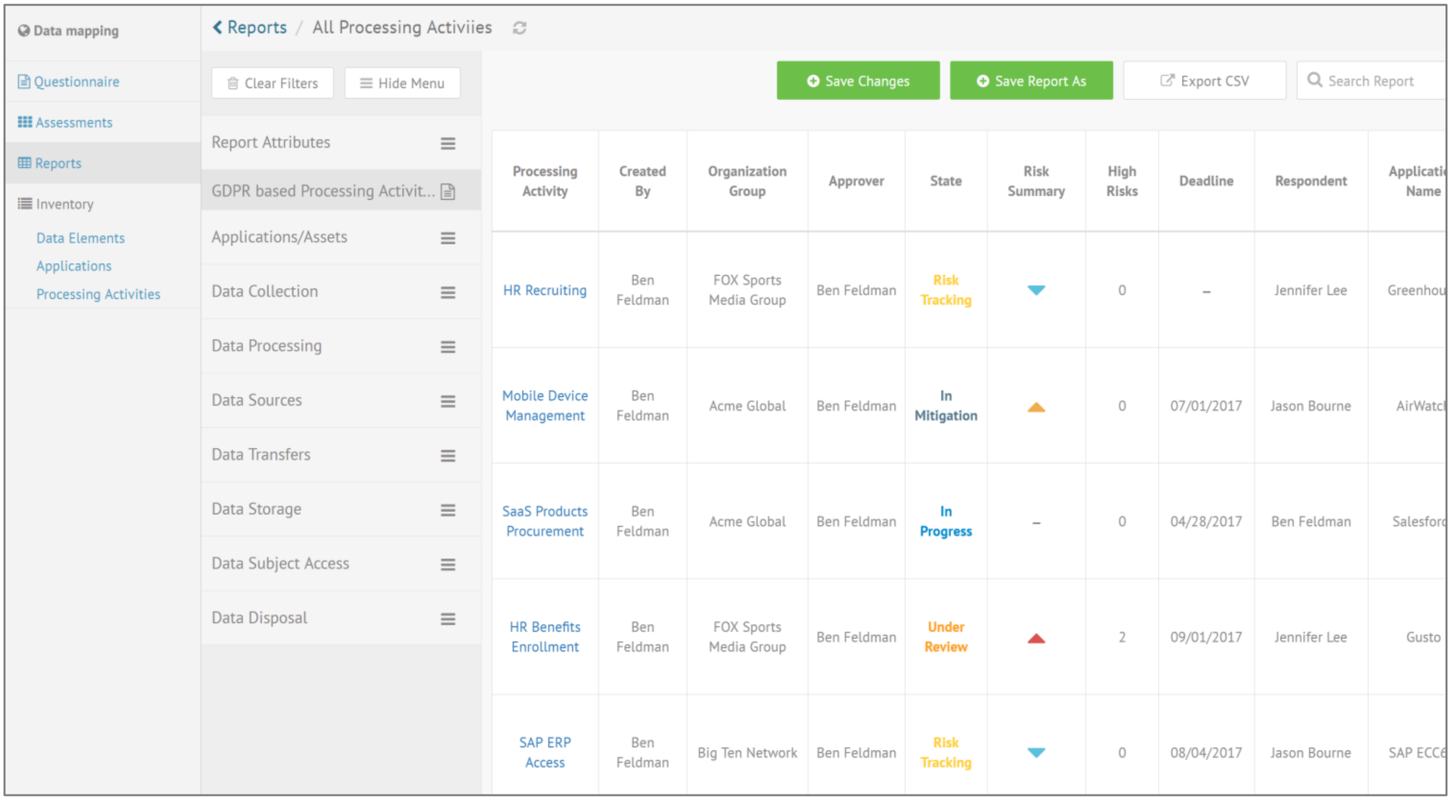
What is a Data Inventory and a Data Map?

Data Inventory

A data inventory is a record of the data flows and assets that an organisation handles. A data inventory is typically organized according to the data lifecycle of collection, processing, transfers, storage, protection, and retention – or another similar framework.

A data inventory is typically formatted in a tabular or Excel-based representation.

Sample data inventory from OneTrust included below:



Processing Activity	Created By	Organization Group	Approver	State	Risk Summary	High Risks	Deadline	Respondent	Applicati Name
HR Recruiting	Ben Feldman	FOX Sports Media Group	Ben Feldman	Risk Tracking	▼	0	–	Jennifer Lee	Greenhou
Mobile Device Management	Ben Feldman	Acme Global	Ben Feldman	In Mitigation	▲	0	07/01/2017	Jason Bourne	AirWatc
SaaS Products Procurement	Ben Feldman	Acme Global	Ben Feldman	In Progress	–	0	04/28/2017	Ben Feldman	Salesforc
HR Benefits Enrollment	Ben Feldman	FOX Sports Media Group	Ben Feldman	Under Review	▲	2	09/01/2017	Jennifer Lee	Gusto
SAP ERP Access	Ben Feldman	Big Ten Network	Ben Feldman	Risk Tracking	▼	0	08/04/2017	Jason Bourne	SAP ECC6

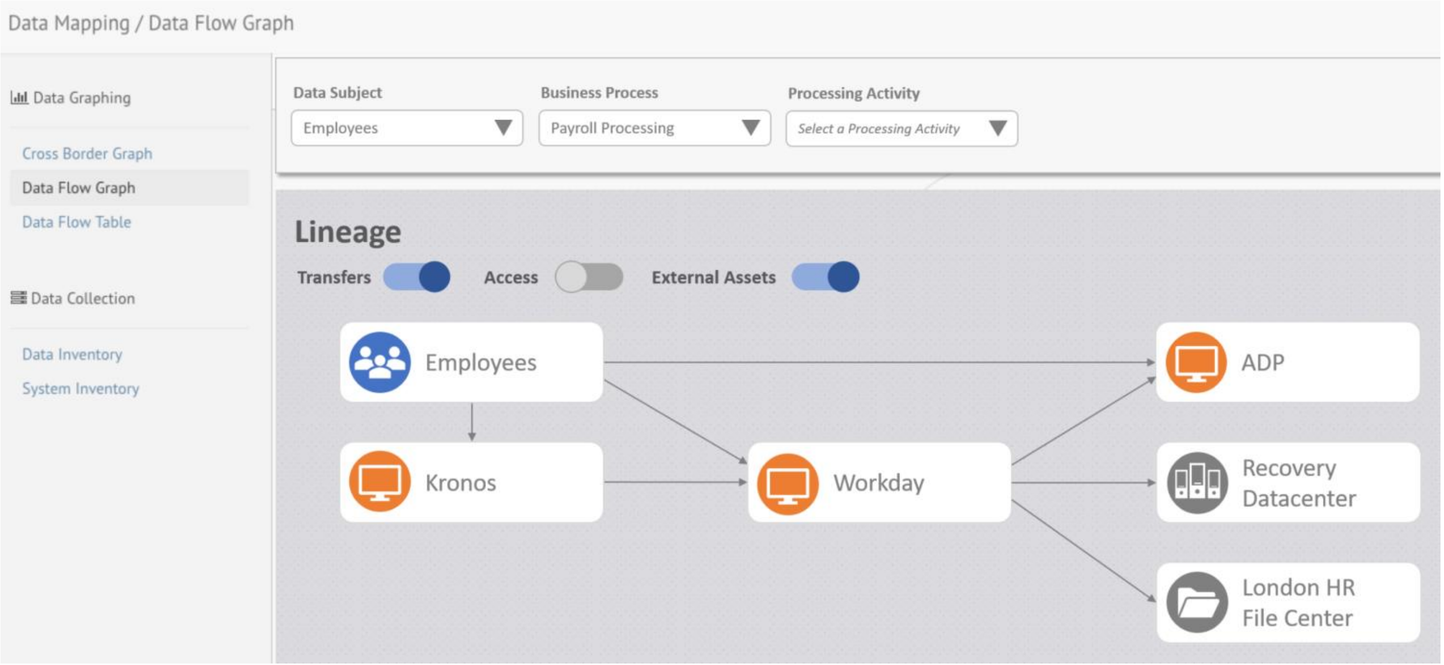
Data Map

A data map is a visual representation of the data inventory. It is generated based on the same underlying data inventory, and the maps may contain varying degree of detail.

Some maps are manually generated using Microsoft Visio, and some can be automatically generated using tools like OneTrust.

Data maps usually focus on representing the data flows and cross-border data transfers. Data maps can also visually indicate and highlight high risk processing of data

Sample data map from OneTrust included below:



Data Mapping / Data Flow Graph

Data Subject: Employees

Business Process: Payroll Processing

Processing Activity: Select a Processing Activity

Lineage

Transfers: on

Access: off

External Assets: on

Personal Data vs. Non-Personal Data

Depending on the drivers for your organisation creating a data inventory or map, it may strictly be a "Personal Data Map" or it may be a more general "Data Map"

Personal data maps are commonly driven out of the need to comply with data privacy regulations like the GDPR, and are limited in scope to only personal data. The records are created with demonstrating accountability in mind.

General data maps that include both personal and non-personal (business confidential, IP, trade secrets, roadmaps, etc.) information are typically driven out of security or information governance functions as well.

How Data Inventory and Maps Are Used

Data maps can be used for a variety of different reasons including:

- **Compliance:** GDPR Article 30 and other regulations require records of processing activities, where the most popular methods of meeting this requirement are data inventories and maps.
- **Privacy statements:** To make privacy statements accurate based on what the organisation is doing.
- **Security**: Understanding where the data is located and flowing is the first step to understanding risk to data which allows the proper security safeguards to be put in place.
- **Responding to customer requests:** Customers may ask what data is your product collecting and where is it being sent. Having a data map makes this easier to reply in a standard way.
- **Responding to data subject requests:** GDPR Article 15 gives individuals the ability to request to correct, port, delete, and access the data that you have about them. Maintaining a central record makes fulfilling these requests much easier.
- **Data breach preparation and response**: Having a data map can help respond more appropriately to a breach and understand what data may have been exposed based on which applications were impacted by a breach.
- **Cost Savings from Consolidation & Minimization:** Mapping your data can also result in the discovery of duplicate data and inefficient business processes that can be streamlined.
- **Increasing business value:** Identifying data that was unknown may reveal new opportunities to use the data.

GDPR Article 30 Requirements for Data Mapping

Although data inventory and mapping is not explicitly mentioned in those words in GDPR, it is widely recognized that Article 30 in the GDPR in practice requires an organisation to do a data inventory and mapping exercise, and most importantly, keep it up to date.

Article 30 Has Specific Requirements for the "Records of Processing Activities"

The most common pitfall in data mapping is that a lot of hard work is done to generate the inventories and maps, however they do not contain the required records of processing activities! This is very common when data mapping and inventory exercises are driven out of IT, Security, or Information Governance teams rather than legal teams.

It is critical to consider the specifics of GDPR Articles 30 and 34 when creating the data maps.

Additionally, many organisations who have been doing data mapping because of PCI, BCR, or Information Governance requirements may assume that their existing data maps meet the GDPR requirements. This is also not correct – data inventories and maps must be revisited to make sure the specific obligations in GDPR are covered.

The relevant Articles and Recitals in GDPR are:

- Article 30
- Recitals 13, 39, and 82

Organisations with Less than 250 Employees May Be Excluded

The "Article 30 record" requirement DOES NOT apply to companies with less than 250 employees UNLESS:

- the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, OR
- the processing is not occasional, OR
- the processing includes special categories of data (= sensitive data - see Article 9(1)) or personal data relating to criminal convictions and offences (see Article 10)

Records Must Be in Writing, Preferably Electronic

- The records must be in writing (electronic form is acceptable) – Article 30(3).
- Organisations must make the record available to a supervisory authority on request – Article 30(4).

Additional Articles to Account for Such as Subject Rights, Security, and Transfers

It might then be useful to capture elements in your data mapping that go beyond those specified in Article 30 (not to show on the Article 30 report, but as a way of meeting other obligations) because controllers and processors (under the GDPR) are obligated to demonstrate compliance with the whole Regulation.

Article 15: Subject Rights

Ex: controllers are responsible for ensuring data subjects' rights (e.g. right of access, right to object)

- Those specific elements are not expressly mentioned in Article 30, so that they do not have to be shown in controller or processor's report

Article 32: Security of Processing

Article 32 is referenced in the requirements of Article 30.

Article 49: Data Transfers

Article 49 is referenced in the requirements of Article 30.

Data Maps for Controllers vs. Processors

The contents of the records may be slightly different for controllers vs. processors.

Article 30(1) outlines requirements for Controllers, and Article 30(2) outlines requirements for Processors. Below is a comparison of the two.

	Controllers (Article 30(1))	Processors (Article 30(2))
Records of What	**Processing Activities**	**Categories of Processing Activities** carried out on behalf of a controller
Contact Info	Name and contact details of: • Controller • Where applicable, the joint controller • The controller's representative • The data protection officer (DPO)	Name and contact details of: • The **processor** or processors • Each **controller** on behalf of which processor is acting • Where applicable of the controller and processors **representatives** • **DPO** (if any)
Purpose of Processing	The **purposes** of the processing	n/a
Data Subjects	A description of the **categories of data subjects**	n/a
Personal Data	A description of the **categories of personal data**	n/a
Recipients	The **categories of recipients** to whom the personal data have been or will be disclosed including recipients in third countries or international organisations	n/a
Security	Where possible, a general description of the **technical and organisational security measures referred to in Article 32(1)**	Where possible, a general description of the **technical and organisational security measures referred to in Article 32(1)**
Cross-Border Transfers	Where applicable, transfers of personal data to a third country or an international organisation Safeguards on the transfer from list in Article 49(1)	Where applicable, transfers of personal data to a third country or an international organisation Safeguards on the transfer from list in Article 49(1)

	Controllers (Article 30(1))	Processors (Article 30(2))
Retention	The envisaged time limits for erasure of the different categories of data	n/a

Additional GDPR Guidance Provided by Regulators

German Working Group

The information below is credited to the following blog entry:

http://www.alstonprivacy.com/german-dpas-create-model-processing-records-gdpr-compliance/

The DPA for the German state of Bavaria issued a circular discussing Article 30 GDPR's new recordkeeping requirements. As Daniel Felz stated in the Alston & Bird Privacy & Data Security Blog that make points are that:

- Article 30 GDPR introduces a major change: not just controllers, but also ***processors*** must maintain processing records and produce them to DPAs upon request;
- Company-maintained processing records will displace the present regime of DPA notifications for certain processing operations and transfers;
- Companies operating in Germany are already generally obligated to maintain an "index of processing activities" (***Verfahrensverzeichnis***), which can serve as a basis for generating GDPR processing records;
- Failure to maintain processing records is subject to fines of € 10 million or 2% of worldwide annual turnover, as is the failure to produce processing records to DPAs upon request.

Seventeen German DPAs have formed a working group that will develop a **Model Processing Operations Index** for Article 30 compliance. The Model Processing Operations Index will likely be released in mid-2017.The Index may become the baseline for DPAs throughout the EU. The Index will also provide the first instance of guidance on the acceptable format for the information processing records kept to meet the requirements of Article 30.

Article 29 Working Party Guidance

As of the publishing of this guide, the Article 29 Working Party is still finalizing their official guidance. Contact OneTrust at support@onetrust.com for an up to date version of this handbook that includes the latest guidance.

Additional GDPR Guidance Expected

Additional guidance from various member states is expected soon. Contact OneTrust at support@onetrust.com for an up to date version of this handbook that includes the latest guidance.

Pre-GDPR Guidance

Some jurisdictions, such as Germany, required record keeping in their local data protection act prior to the GDPR. These jurisdictions have some guidance available that may be valuable for companies located in these specific jurisdictions as well.

BCR Requirements for Data Mapping

Organisations who participate under the Binding Corporate Rules (BCR) program also have requirements for data mapping. A summary of those are included here:

- Overview on Binding Corporate rules
    - http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm
- BCR Checklist
    - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf

Description of Processing and Data Flows

The below is the relevant portion of the BCR obligations that results in a data mapping requirement. If an organisation has BCR, or plans to do BCR in future, these specific record obligations should be incorporated into the map.

> 4 - DESCRIPTION OF PROCESSING AND DATA FLOWS
>
> 4.1 A description of the transfers covered by the BCRs
>
> The BCRs must also contain a general description of the transfers to allow the Data Protection Authorities to assess that the processing carried out in third countries is adequate and more precisely on: i) the nature of the data transferred ii) the purposes of the transfer/processing iii) the data importers/exporters in the EU and outside of the EU Some Data Protection Authorities may require more detailed description of the transfers.
>
> 4.2 A statement of the geographical and material scope of the BCRs (nature of data, type of data subjects, countries)
>
> The BCRs should indicate if they apply to: i) all personal data transferred from the European Union within the group OR, ii) all processing of personal data made within the company group The BCRs must also specify its material scope, for instance, that the BCRs apply to personal data related to employees, customers, suppliers and other third parties as part of company's regular business activities.

Information Governance Requirements for Data Mapping

Many organisations have a centralized information governance team that may be maintaining central data maps.

Many of these teams are focused on both personal and non-personal information, and use scanning tools build for information security and data governance use cases.

These tools in practice may not have been designed to meet the specific obligations of GDPR, and privacy professionals are encouraged to get into the details of the specific records that these tools collect, and advise the information governance teams that GDPR does not simply require a data map, but requires specific records of processing activities. This document can be used as a reference for these teams.

Tools built for GDPR, such as OneTrust, can integrate with these data governance tools to provide a robust overall program both for privacy professionals as well as information governance teams.

Non-EU: Requirements and Specific Guidance in Other Jurisdictions

Canada

- "Personal Information Inventory" described here:
- https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/gl_acc_201204/

Other jurisdictions also provide requirements that are being indexed and compiled in future versions of this document.

Part 2: The Ten Steps to Meet GDPR Article 30

Under the EU GDPR, which goes into effect on **May 25, 2018**, organisations will be expected to maintain extensive records of their personal data processing activities, which will require a granular level of detail that has not been previously required.

One way to comply with the new regulation is through data mapping, a process by which organisations develop and maintain a visual documentation of their data journey, helping them more tightly control internal and external data flows, mitigate privacy risks, and increase operational efficiencies.

To help your organisation prepare for GDPR, OneTrust has developed a systematic guide to data mapping that will support your decision-making and set you on the right path toward compliance with record keeping requirements.

ONE | Determine What You Already Have

Many organisations already have some form of data maps or records of their assets that contain personal data. These sets of information are often fragmented across departments, contain varying levels of detail, and they typically don't meet Article 30 requirements for two reasons:

1. IT-focused data maps typically include detailed network and infrastructure information but lack details on the subjects and categories of personal data being processed
2. Existing maps are not usually organised by data processing activities

Companies should start by deciding what data can be extracted and repurposed from their existing data maps. Key things to look for in existing documentation are:

- Lists of assets (applications, databases, file systems) and their location
- Defined business processes and sub-processes which handle personal data
- Lists of third parties that are used to help with the processing of personal data

TWO | Decide What Attributes are Needed in the Inventory

To produce a data map that complies with GDPR Article 30, companies must ask themselves and document the following basic questions about how they collect, use, and transfer personal data:

- What type of personal data is collected?
- How, and from where, is the data collected?

- How and where is the data processed?
- How and where is the data being transferred?
- Is the data being stored, protected, and deleted?

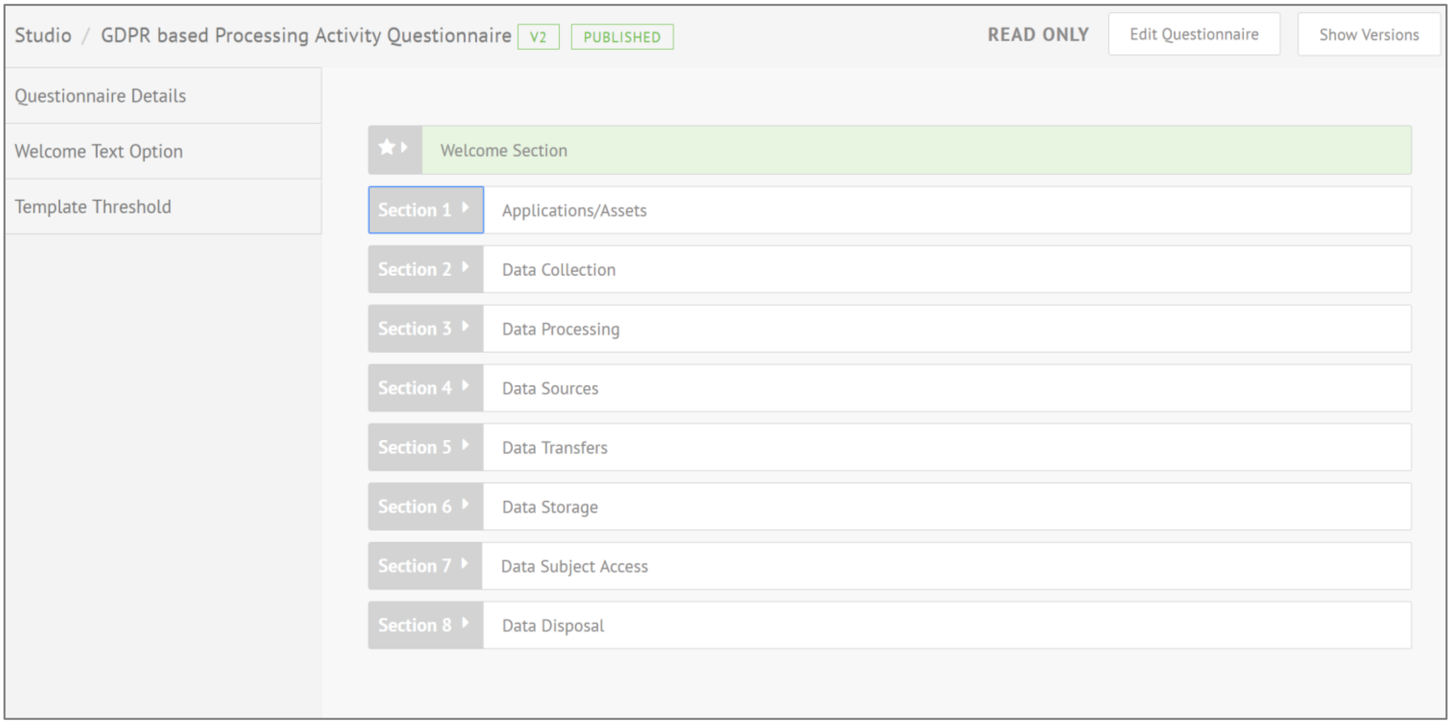
Part 1 of this handbook covered the requirements for data mapping in detail.

While answering and documenting these questions will result in a GDPR Article 30 compliant records or processing activity, most organisations choose to document additional information in their data maps. This further documentation is performed in tandem because a well-maintained data map is often the easiest place to ensure your processes follow other GDPR Articles.

A few of the most common GDPR Articles that are documented within a company's data map are:

- **Article 7:** regarding conditions for and proof of consent
- **Articles 15-19:** regarding the rights of the data subject
- **Article 20:** regarding the portability of the data contained in the asset
- **Article 30:** records of processing activities
- **Article 32:** regarding security measures
- **Articles 44-46:** regarding transfers of personal data

Below is a sample of a template and standard questionnaire that comes with the OneTrust data mapping software.



Welcome Section

Section 1 Applications/Assets

Section 2 Data Collection

Section 3 Data Processing

Section 4 Data Sources

Section 5 Data Transfers

Section 6 Data Storage

Section 7 Data Subject Access

Section 8 Data Disposal

THREE | Mapping Applications vs. Business Processes

Now that you have identified what you have, and where you want to get to, you likely have a list of gaps between the current state and end state. You may even be starting from scratch.

The question now becomes what do you populate those attributes for? What is the "thing" to map?

In general, there are two ways of thinking about this:

Application Centric-Map:

An application centric map is common for IT driven teams. You compile a list of the applications in the environment, along with the IT and business owners of those applications. You then send out the questionnaire that you've created to those owners, or scan and identify data based on each application.

Since GDPR also requires processing activities, when doing application-centric data maps, be sure to capture an attribute for the application for the processing activities and purposes of processing. There can be multiple processing activities for an application.

Processing Activity/Business Process Centric-Map:

Many times, when the mapping exercise is driven more from a legal initiative, the mapping is done based on business processing activities. For example: "Recruiting process" "Quote to Cash Process" "Performance Management Process", rather than each individual IT application. The IT application(s) involved with the process are then captured through the questionnaire that is sent on the processing activity.

Different Means to the Same End

Processing activities and applications are related, and if the tool you are using to do the mapping is intelligent enough to create these relationships, then the result is the same regardless if you map on apps or processes. Most companies map on apps; however, it is not uncommon to take a hybrid approach.

Generating the List of Apps or Processes

Many organizations have some existing technologies that hold existing lists of apps or processes and can be a great starting point to import into your data mapping tool to send the data mapping questionnaire against those apps:

CMDB: "Configuration Management Database" is a generic term for an inventory of applications or systems that an IT organization is dealing with. Common CMBD technologies include:

- ServiceNow
- BMC Remedy
- GRC such as RSA Archer
- Application Portfolio Management Tools

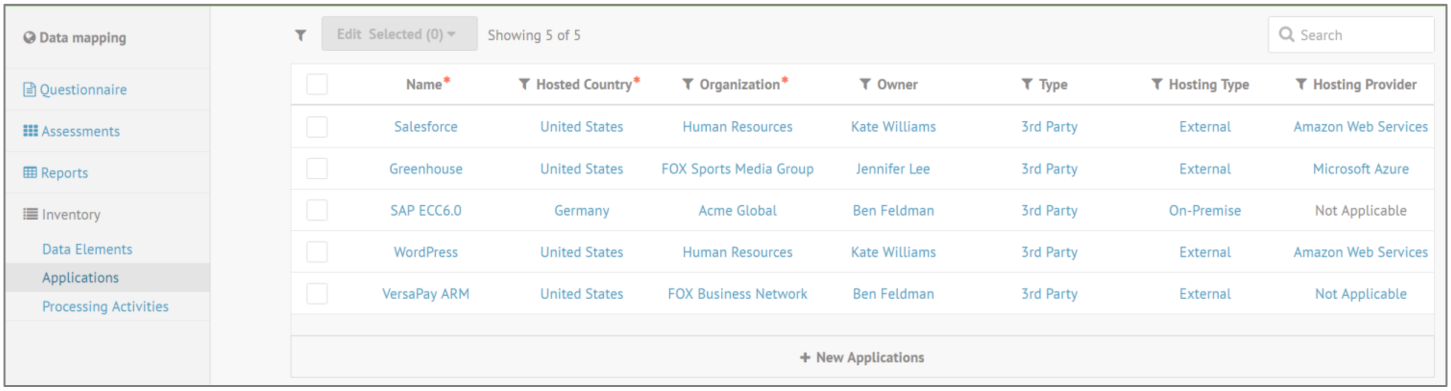
GRC: “Governance Risk Compliance” tools are used by central compliance teams and sometimes have a list of processes that have been inventoried that can be used.

If you are starting from scratch, then the most common way to generate the list is from a combination of interviews and workshops in person with key groups and stakeholders to get the initial lists. Some scanning technologies may be able to be used, but in practice results vary with scanning, and implementation times for scanning technologies may introduce delays in the mapping exercise.

Additionally, your tooling or consulting vendor may have an existing list of common applications and processes in organizations you can start from.

OneTrust provides the ability to map based on either processing activities or applications, and is flexible to be used in a hybrid approach. Apps and processes can be re-used and shared across different legal entities or organization groups in OneTrust.

Additionally, the interface is built in a way to facilitate note taking and fast record keeping when in interview or workshop type formats. The tool can be integrated into your GRC or CMDB directly via APIs, or also through an export import.



Showing 5 of 5

Name*	Hosted Country*	Organization*	Owner	Type	Hosting Type	Hosting Provider
Salesforce	United States	Human Resources	Kate Williams	3rd Party	External	Amazon Web Services
Greenhouse	United States	FOX Sports Media Group	Jennifer Lee	3rd Party	External	Microsoft Azure
SAP ECC6.0	Germany	Acme Global	Ben Feldman	3rd Party	On-Premise	Not Applicable
WordPress	United States	Human Resources	Kate Williams	3rd Party	External	Amazon Web Services
VersaPay ARM	United States	FOX Business Network	Ben Feldman	3rd Party	External	Not Applicable

FOUR | Questionnaires vs. Network Scanning

Once you’ve decided what you are going map, you need to determine how you will gather the information. There are a few methods you can use to populate your data map:

- Questionnaires
- Automated Scanning
- API Integrations (Feeds from other systems)

Questionnaires: This method can effectively fulfill GDPR Article 30 requirements. Its shortcoming is that it does not help organisations incorporate data they are not aware of.

Data Discovery (Automated Scanning): This method may be able to tell you the data location, volume, encryption, and rough classification. Scanning alone does not capture enough information to meet the Article 30 record keeping requirements as it is not able to provide information regarding the purpose of processing and other contextual details. Also, scanning requires significantly more IT sponsorship and ownership to execute than the other methods described in this step.

APIs: Many companies have existing inventories of assets or vendors, but those inventories usually do not include all data flows associated with them. Even though more information is necessary, if you have existing inventories, you'll want to reuse them. This is where API integration can help. You can integrate your data mapping tool with existing IT systems that store information on assets such as applications and databases.

Most companies prefer to start with a combination of API and questionnaire-based approach. This allows them to first build an inventory of existing assets then send questionnaires out for each asset. Automation can be implemented over time to keep data current once it is already populated.

OneTrust supports all three approaches. Questionnaire, automated scanning, and API capabilities are all available.

FIVE | Scoping & Prioritizing Organisation Groups

It's important to involve stakeholders across departments early in your conversations about data mapping. Doing so can help you determine which groups must be included and promote collaboration among their teams, as well as help you identify and train privacy champions across organisations. These champions will be vital in determining the scope of what needs to be mapped in each organisation.

- Potential groups may include: HR, Marketing, Procurement, Customer Success, and others
- Sample questions to ask your teams may include:
    - How is the marketing team capturing leads?
    - How is the recruiting team collecting new hire information?
    - How is the procurement team vetting new vendors?

Think about where you can start small with potential to expand, and consider any teams with which you already have a relationship. You may also find that certain teams are more amenable to data mapping cooperation, depending on the level of enforcement of privacy regulations in their respective markets.

Practical considerations to think about:

- Leverage personal relationships and start a POC with a "friendly" group that sees the value in the map

- Starting complex vs. simple come with different opinions. Some organizations like to start complex with the most difficult teams and use cases to make sure they have a stake in the process, their feedback can be included, and that future teams will be easy. Others like to start simple and work their way up.

You'll likely find that your company has a lot of different assets that contain personal data. Some may require mapping and others may not. To complete your data map, you must start somewhere. It's best to prioritize what you'll map as this will be critical when you start to assemble your project team. You should consider the following during the prioritization process:

- Scale of processing
- Sensitivity of personal data being processed
- Risk for data breach
- Organisational/Departmental ability to provide the required information

Most companies select a subset of organisations or departments to start with. Within those groups, they prioritize each process by their combined scale or processing, sensitivity of data, and risk of breach.

OneTrust has a grouping hierarchy capability that allows you to setup legal entities, countries, and business functions in a matrixed approach to scope and prioritize rolling out the data mapping initiative.

SIX | Project Staffing

Designing, implementing, and maintaining data maps involves an organisation's Privacy Office, legal, IT, and records management staff. Some companies engage outside consulting companies to assist with and organize the data mapping process in addition to their internal staff members.

Regardless of how you choose to staff your data mapping project, the key to success is to establish standards and implement tools that ensure an evergreen level of consistency with your data mapping efforts.

Equally as important is to identify privacy champions within the organisation who support your privacy program, and can serve as advocates for fostering privacy as a core company value.

Usually a business or IT owner is assigned to the process or application to map, and they are sent the questionnaire and responsible for the completion. That person can then sub-delegate out sections if needed. The privacy champion for this person's team is a point of contact to help identify the owner, as well as support the owner with any privacy specific questions without overburdening the central privacy office or data mapping project manager.

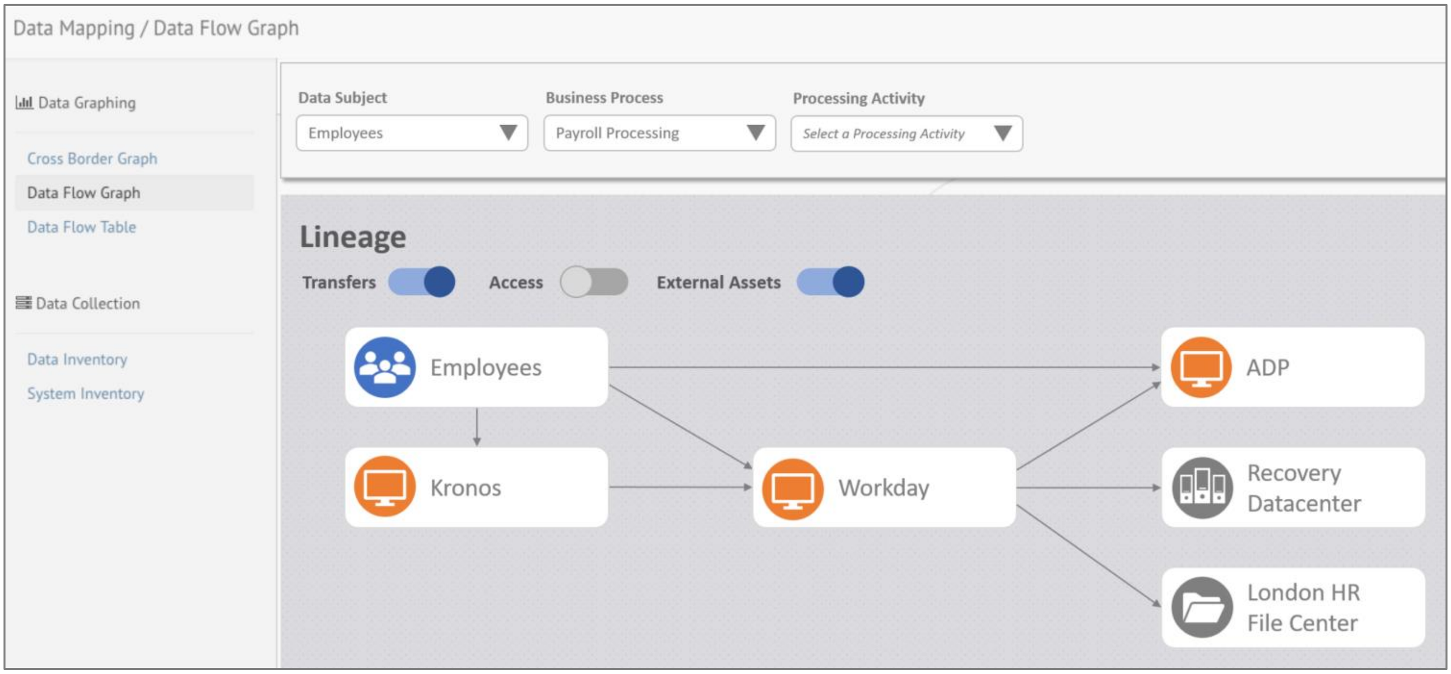
SEVEN | Reporting

Consider how your privacy team, peers across Security and IT teams, and/or superiors prefer to digest data maps. Each group will likely require different levels of detail when reviewing data mapping reports.

Most companies start with tabular reports since this is the easiest way to demonstrate compliance with Article 30. To facilitate internal discussion and research, many companies rely on visual reports such as asset-tracking maps, cross-border data transfers maps, or data lineage diagrams. Visual reports like these allow companies to overlay risks and control gaps visually on data maps to quickly identify areas that need attention.

After deciding which reports you'll use, you should revisit the attributes you've decided to gather to ensure you're collecting everything you need to construct your visuals. Regardless of format you choose, you must make sure that your reports are meeting the GDPR record keeping requirements that are outlined in Article 30 (see full text below).

OneTrust supports both a spreadsheet based tabular report, as well as visual reports. Samples are included below:



Data Mapping / Data Flow Graph

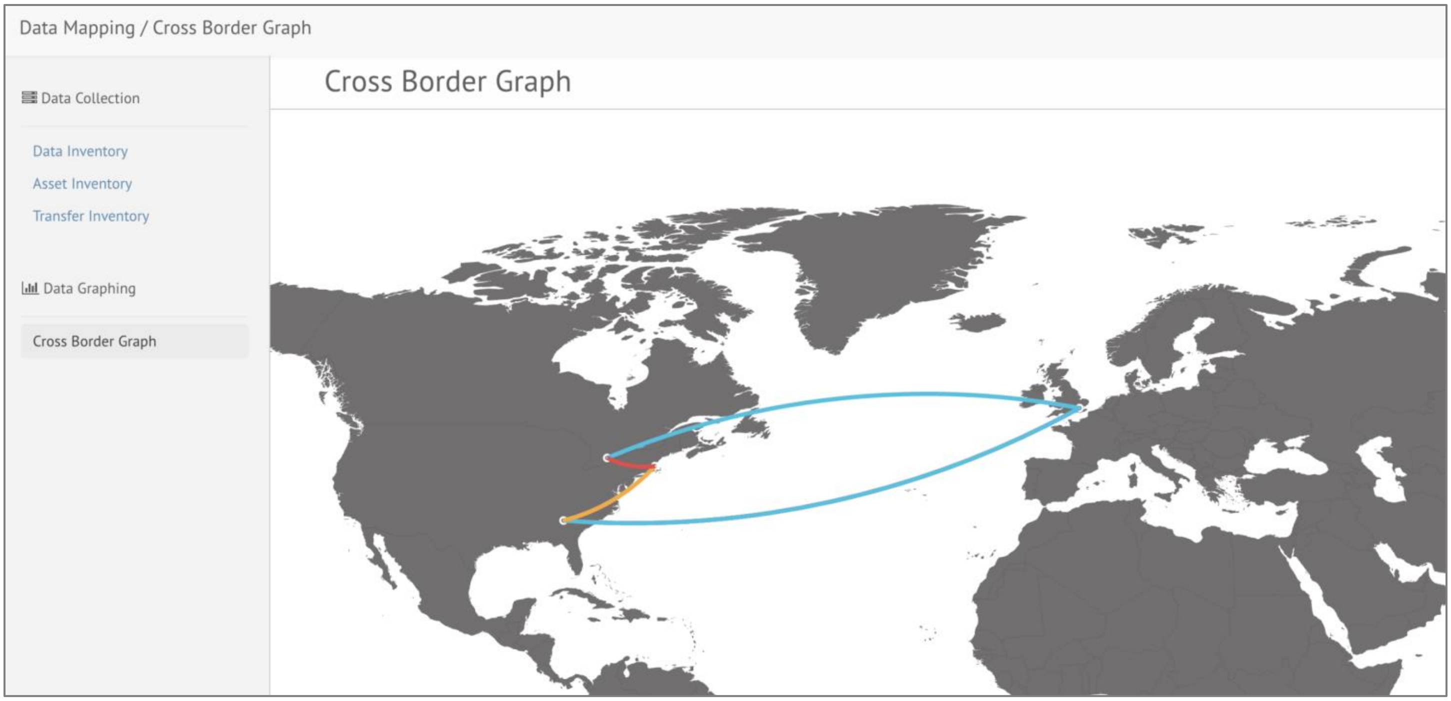
Data Subject: Employees

Business Process: Payroll Processing

Processing Activity: Select a Processing Activity

Lineage

Transfers ● Access ○ External Assets ●

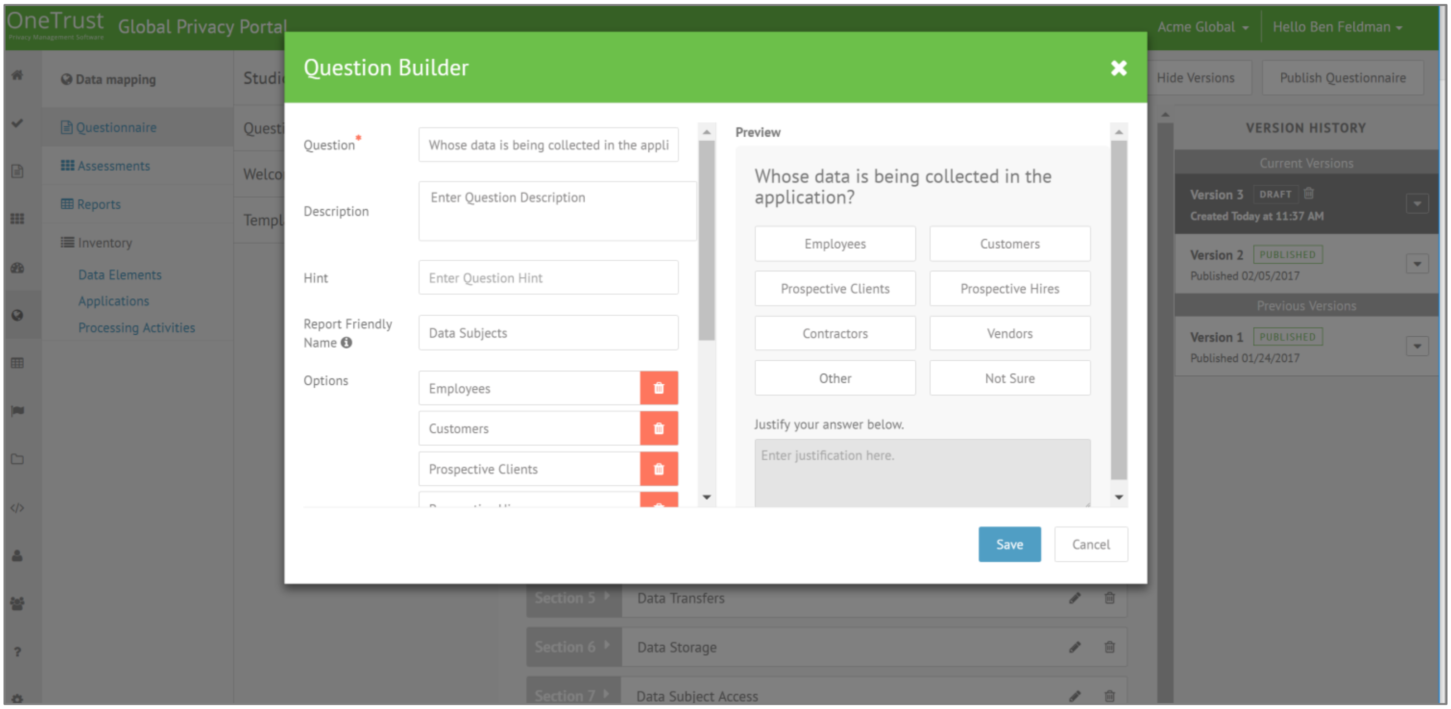


EIGHT | Full Scale Roll Out and Continuous Improvement

After you've identified what you're mapping, the methods you'll use, and the project team that will be helping, you're ready to start filling out your data map. To ensure that the map you're building is accurate a review and approval process should be put in place for all the data that is feeding into your map. This process should allow Privacy Officers to review each incoming questionnaire, API feed, or scanning results to ensure its information is accurate before it is added to the register.

All data being added to the data map should have history tracking to show who provided, modified, and approved the information. This is critical when it comes to resolving conflicting accounts about similar processes or assets.

OneTrust supports version management on the questionnaires so you can edit, modify, and add new versions at any time while maintaining the historical data.



Question Builder

Question*: Whose data is being collected in the appli

Description: Enter Question Description

Hint: Enter Question Hint

Report Friendly Name: Data Subjects

Options: Employees, Customers, Prospective Clients

Preview

Whose data is being collected in the application?

Employees | Customers | Prospective Clients | Prospective Hires | Contractors | Vendors | Other | Not Sure

Justify your answer below.

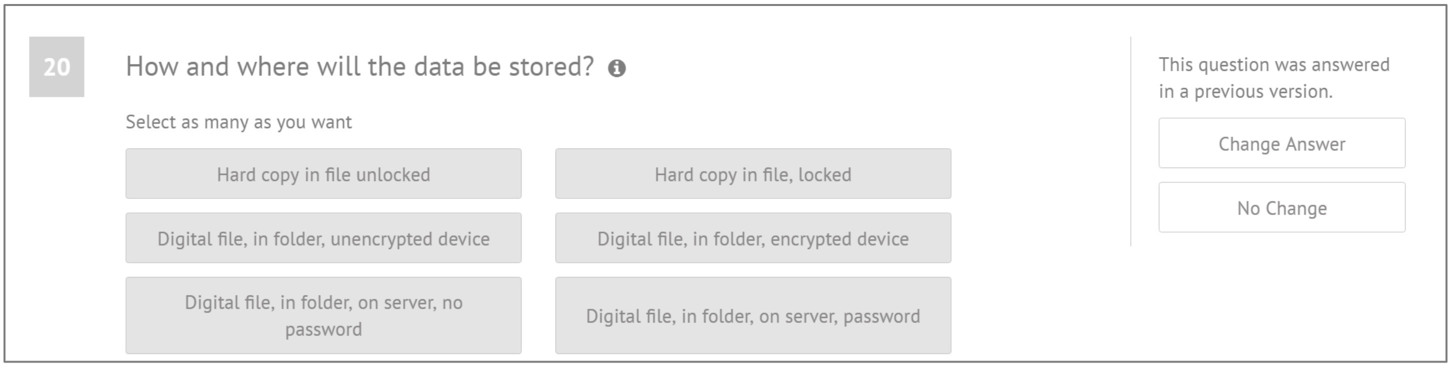
Enter justification here.

NINE | Keeping Your Data Map Current

After you've updated your data map to a point that you have deemed current, you will need to have a plan for how to maintain it. It is critical to use a tool to keep the maps current. Tools can help in several ways:

1. Automated "What changed" audits are the most common way to keep the maps up to date. Based on risk, some data flows or apps may be re-audited on different time scales. When sending the audit questionnaire, instead of asking all the same questions over again, a best practice is to just ask "what changed" for each question.
2. Ongoing PIA and Risk Assessments on new projects feeding into the data inventory
3. Ongoing Vendor assessments feeding into the data inventory
4. Automated tool to keep the visual maps up to date dynamically based on the changes to the underlying inventory
5. Automated scanning tools deployed in parallel to detect any changes in data

Sample of a "what changed" re-audit workflow in OneTrust:



20 How and where will the data be stored?

Select as many as you want

- Hard copy in file unlocked
- Hard copy in file, locked
- Digital file, in folder, unencrypted device
- Digital file, in folder, encrypted device
- Digital file, in folder, on server, no password
- Digital file, in folder, on server, password

This question was answered in a previous version.

TEN | Choose a Tool That's Right for You

Data mapping requires an investment of time and resources, choosing the right technology can help maximize the results you see. In selecting a vendor for your data mapping needs, one of the primary distinctions among solutions is the level of integration with your various privacy workflows.

Choosing a stand-alone data mapping tool versus a comprehensive privacy management platform has a significant impact on your ability to operationalize compliance with record keeping requirements. Besides the technology, itself, it's important to consider the ease of implementation and use, as you scale this across your privacy network.

OneTrust provides a fully-integrated approach to data mapping that makes it easier for organisations to visualize their data flows and to maintain compliance with GDPR regulations.

Templates Available as Starting Points

OneTrust provides many different types of data inventory and mapping templates.

These templates include conditional logic rules, embedded help and training, and have been created by privacy experts around the world.

Contact OneTrust at support@onetrust.com for access to these templates.

Reference: GDPR – Article 30 (Full Text)

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all the following information:
    a. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer;
    b. the purposes of the processing;
    c. a description of the categories of data subjects and of the categories of personal data;
    d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
    e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
    f. where possible, the envisaged time limits for erasure of the different categories of data;
    g. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
    a. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
    b. the categories of processing carried out on behalf of each controller;
    c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
    d. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

About OneTrust

OneTrust is the leading and fastest growing privacy management software platform used by over 1,000 organisations globally to comply with data privacy regulations across sectors and jurisdictions, including the EU GDPR and Privacy Shield.

Our comprehensive, integrated, technology-based solutions include readiness and privacy impact assessments, data inventory and mapping, automated identity and data discovery, website scanning and cookie consent management, subject rights and consent management, incident reporting, and vendor risk management.

The OneTrust platform is pre-configured with templates and workflows that can be easily tailored via our point-and-click UI based on unique industry and organisational requirements. We make it easy for privacy teams to get started with OneTrust by giving them the flexibility to upgrade platform capabilities as their program matures, deploy in the cloud or on premise, and scale to support a growing network of privacy champions.

OneTrust is based in Atlanta, GA and London, UK with a team of local privacy and technology experts across North America, Asia, and Europe.

OneTrust is backed by the founders of Manhattan Associates (NASDAQ: MANH) and AirWatch ($1.54B acq by VMWare).