Hopex Privacy Management

User Guide

Bizzdesign

Hopex Aquila

CONTENTS

Contents

INTRODUCTION TO HOPEX PRIVACY MANAGEMENT

Hopex Privacy Management is a solution which helps you manage your compliance to data-protection laws such as the GDPR.

The solution provides a collaborative workspace for DPOs and cross-functional stakeholders.

With this solution you can produce the required documents to prove that you have control over personal data privacy and that you adopted the necessary security measures.

Hopex Privacy Management integrates up-to-date regulatory details and legal templates to accelerate your remediation plans.

Hopex Privacy Management enables you to reuse org-units, processes and applications created in **Hopex Business Process Analysis**, **Hopex IT Architecture** and **Hopex IT Portfolio Management**.

Pre-Requisites to Hopex Privacy Management

The ***first time*** you install **Hopex Privacy Management** you need to import the Privacy Management Content module (hopex.privacy).

To import a module, see Importing a Module into HOPEX.

CONNECTING TO HOPEX PRIVACY MANAGEMENT

To connect to **Hopex Privacy Management**:

1. Start the **Hopex** application using its HTTP address.

   ☛ *If you do not know this address, contact your administrator.*

   The connection page appears.
2. In the **Login** field, enter your identifier.
3. In the **Password** field, enter your password.
4. In the drop-down menu for environments, select your work environment.

   ☛ *If you can access one environment only, this is automatically taken into account and the environment selection field does not appear.*
5. Click **SIGN IN**.
   When you have been authenticated, a new dialog box appears.
6. In the drop-down menu for repositories, select your work repository.

   ☛ *If you can access only one repository, this is automatically taken into account.*
7. In the profile drop-down menu, select the profile with which you want to work:
   For more information on profiles, see Profiles used in Hopex Privacy Management.

   ☛ *If you can access only one profile, this is automatically taken into account.*
8. Click **Privacy Policy**, read the confidentiality policy, then select **I have read and accept the privacy policy**.
   The **LOGIN** button is active.

   ☛ *When you have read and accepted the confidentiality policy, a certificate is automatically linked to your person and this step is not required again.*
9. Click **LOGIN**.

   ☛ *Click **BACK** if you want to return to the authentication dialog box.*

   The home page of your desktop appears and a session is opened.

   ☛ *After a certain period of inactivity, you are disconnected from the desktop. To reconnect, repeat the steps of the procedure above. This inactivity period is configured by the portal administrator.*

PROFILES USED IN HOPEX PRIVACY MANAGEMENT

Summary of Profiles

Profiles	Definition
Processing Activity owner	The processing activity owner is an operational agent in charge of the description of the processing activities within his scope of activity (data, data subject, transfer, etc.) He provides a detailed description of the processing activity.
Data Protection Officer (DPO)	The Data Protection Officer (DPO) is an expert on data Privacy who ensures that an entity is adhering to the policies and procedures set forth in the data privacy law. The DPO plays the role of advisor in the company, compliance correspondent to the regulatory authority and first point of contact for data subjects' claims. He: - ensures that all information required is available to the experts. - has rights on all reference data (eg. data categories, security measures). - is responsible for defining the environment. - edits processing activities, carries out pre-assessments as well as DPIAs.
Chief Privacy Officer	The Chief Privacy Officer is the head of the company compliance program and main responsible person for the overall implementation of the compliance program. Together with the DPO, he assigns priorities and assesses risks of the processing activities making sure that the collected data is sufficient to respond to the requirements of the law.
Privacy Team	The Privacy team is made of operational people who carry out the instructions of the DPO or the Chief Privacy Officer. This profile is to be used by any member of the compliance team.

Rights for Hopex Privacy Management Profiles

The Chief Privacy Officer profile can see everything (menus of the application and objects of the repository)

Actions	Processing Activity Owner/ Application Owner	Chief Privacy Officer	DPO/ Privacy Team
Accessing the Privacy Environment (**Key Elements** section) - Data categories - Data subject categories - Sensitive activities - Supervisory authorities - Transfer safeguards - Country adequacy - Security measures - Technologies - Physical archives		X	X
Defining the Organization (**Organization** section) - Legal entities & DPO - Departments - Organizational model - Functions - Third parties - DPO organigram report - Policies & Procedures		X	
Describing Processing Activities (**ROPA** section)	X	X	X
Managing Regulations		X	X
Performing a Pre-assessment **ROPA** section > **Pre-assessment** page of a processing activity - Identifying compliance level - Identifying risk level		X	X

Actions	Processing Activity Owner/ Application Owner	Chief Privacy Officer	DPO/ Privacy Team
Performing Impact Assessment (DPIA) **ROPA** section > **DPIA** page of a processing activity - Defining Risks - Defining Recommendations and Remediation Actions		X	X
Managing Data Breaches **Data Breaches** section		X	X
Managing Data Subject Requests **Data subjects** section		X	X
Action Plans -Managing Action Plans - Submitting Action Plans	X	X	X

USEFUL FEATURES

☛ *For more information on how to use the desktop and repository, see Objects*

Object status

The objects of the environment have statuses in **Hopex Privacy Management**.

Objects of your environment can have a status, which can be:

- **candidate**: to be validated by a DPO / the Privacy team
- **live**: has been validated by the DPO / the Privacy team
- **obsolete**: no longer exists

You can specify the status on the top right-hand side of the object, for example a processing activity.

Collaboration features

Hopex Privacy Management simplifies teamwork and offers different means of communication. You can:

- create and participate in review notes on objects.
- add tags.
- view your activity.
- share with the other **Hopex** users: add tags, like an object.

☛ *For more information, see Communicating in HOPEX.*

REUSING ENTERPRISE ARCHITECTURE DATA

Hopex enables you to reuse data already created in other **Hopex** solutions to build your privacy environment.

You can:

- ✓ convert Hopex EA org-units to organizations
- ✓ reuse processes and applications to create the needed processing activities.

CONVERTING HOPEX EA ORG-UNITS TO ORGANIZATIONS

In **Hopex IT Portfolio Management** and **Hopex IT Architecture**, org-units are used to describe the overall organization. If you want to reuse **Hopex** objects, you may need to convert org-units to organizations so that they are recognized in **Hopex Privacy Management**.

Converting Org-Units to Organizations

To convert org-units to organizations:

1. Select **Integration > Organizations**.
2. Select the org-units of interest to you and click **Convert**.
3. In the wizard that appears, select the type of conversion needed:
   - **Convert to legal entity**

     📖 *A Legal Entity is a company or an organization which has legal rights and obligations.*
   - **Convert to department**

     ☛ *If you select "department", you need to select the legal entity the selected department should be linked to.*
   - **Convert to third party**

     📖 *A Third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.*
4. Click **OK**.

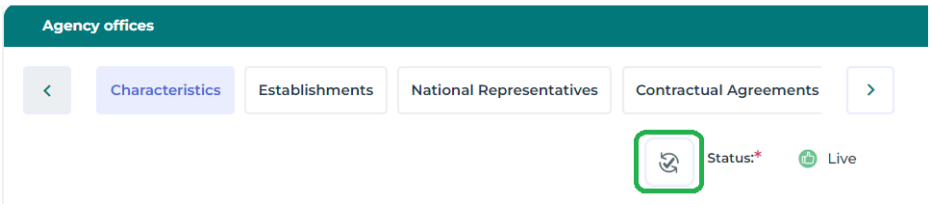
You can view the created legal entities/departments/third parties from the **Organization** menu.

☛ *Technically speaking, the conversion creates a link between the organization and the EA org-unit. The organization inherits from the org-unit local name, which becomes the legal entity/third party/ department name.*

Synchronizing EA-Privacy Organization

When an object is modified in **Hopex**, you can perform synchronization within **Hopex Privacy Management**. In the property page of the organization

corresponding to the modified org-unit, a specific Synchronize button is made available.



To activate this option:

1. From the main menu, select **Settings > Options**.
2. In the **HOPEX Solutions > Privacy Management** section, select "Display the synchronization buttons for Privacy-EA integration".

CREATING PROCESSING ACTIVITIES FROM EA OBJECTS

Hopex Privacy Management enables you to reuse processes and applications from other solutions.

Drag a/an..	to a ...	You obtain:
Process	Department	A processing activity
Application	Department	- A processing activity - Below, a processing element containing the application
Application	Processing activity	- A processing element containing the application

Summary of possible reuse with processes and applications

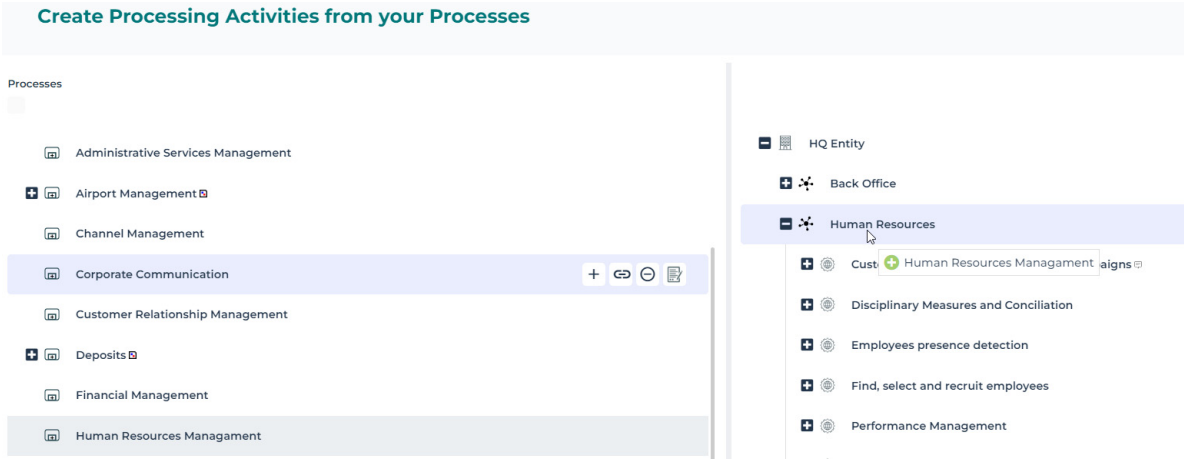
Creating Processing Activities from Processes

You can use a process category or process from other **Hopex** solutions to create a processing activity.

To create a processing activity from a process:

1. Select **Integration > Process Categories**.
   A wizard appears.

2. Select a process in the left tree and drag and drop it to the right tree ***under a specific department***.



A processing activity has been created. You can now access it through the records of processing. For more information see Accessing Processing Activities.

> ☛ *If you have troubles creating a processing activity from a sub-process, you may find it useful to check our FAQs. See About HOPEX Privacy Management Import and HOPEX Integration.*

Creating Processing Activities from Applications

An **Hopex** application can become a processing element in **Hopex Privacy Management**.

> ☛ *For more information, see Managing Processing Activity Elements.*

You can therefore use an application to create a processing element below an existing processing activity.

To create processing elements from applications:

1. Select **Integration > Applications**.
2. Select an application in the left tree and drag and drop it to the right tree ***under a specific department***.

If there is no processing activity right below the department of interest, a processing activity wizard appears. A processing element is automatically created under the processing activity.

The application is automatically linked to the created processing activity (via the processing element).

> ☛ *You can also simply drag and drop an application to an existing processing activity to make a link between them (via a processing element).*

SETTING UP THE PRIVACY ENVIRONMENT

As a Chief Privacy Officer you need to set up the environment, which consists in making sure that predefined lists of objects (for example data categories and data subject categories) are properly defined.

☛ ***Hopex Privacy Management*** *provides default data sets. It is necessary for you to analyze them in order to contextualize these sets to your company needs.*

Accessing the Privacy Environment

To view and modify key elements of your environment:

- Select **Key Elements**.

The most important elements to be defined are:

- Defining Data Categories
- Data Subject Categories.

Under GDPR key elements, you also have access to:

- Defining Sensitive Activities
- Defining Supervisory Authorities
- Defining Transfer Safeguards
- Defining Country Adequacy information
- Defining Security Measures

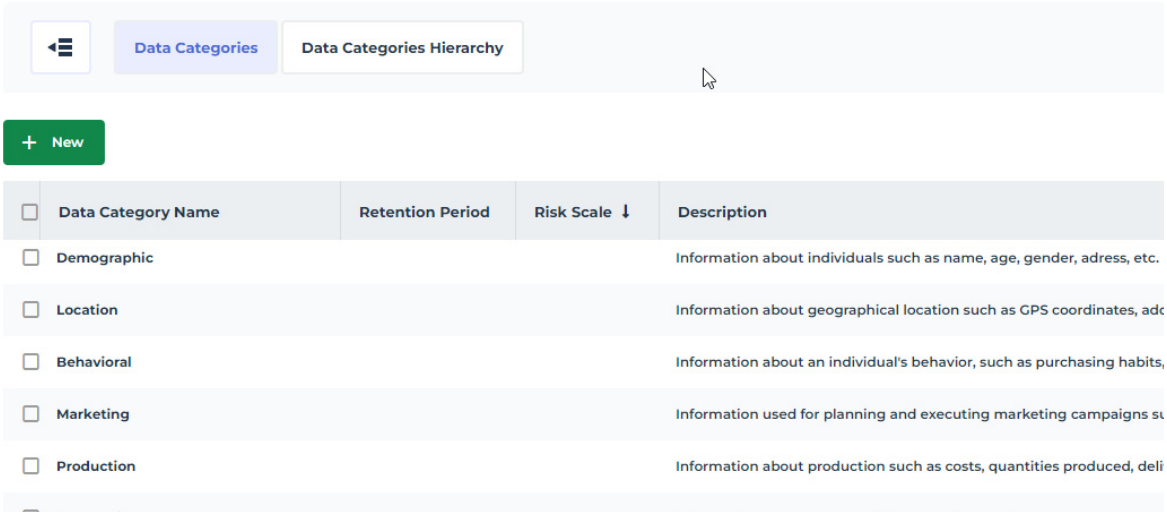
DEFINING DATA CATEGORIES

In **Hopex Privacy Management**, data categories represent categories of personal data.

Proper definition of data categories is crucial to the subsequent description of company processing activities.

To define data categories:

1. Select **Key elements > Data Categories.**
2. Identify the most common personal data categories used in your business processing activities.




```
Below are examples of data categories:
- Contact information: name, address and ID numbers.
- Health data: blood type, physical health status
- Biometric data: Fingerprint, speech recognition
- Sensitive data: race, ethnicity, nationality
```

You can define:

- the **Retention period**: default value referring to how long the organization usually keeps this type of data. This time lapse should not be longer than necessary for the purposes for which the personal data is processed.

  ☛ *This default value gives an average indication of what the retention period might be. The actual retention period must be redefined on*

processing activities, as it depends on the context and objective of data usage.

For more information, see Specifying the retention period on a processing activity.

- the **Risk scale**: default risk level associated to the data category (eg. "high" for financial data).

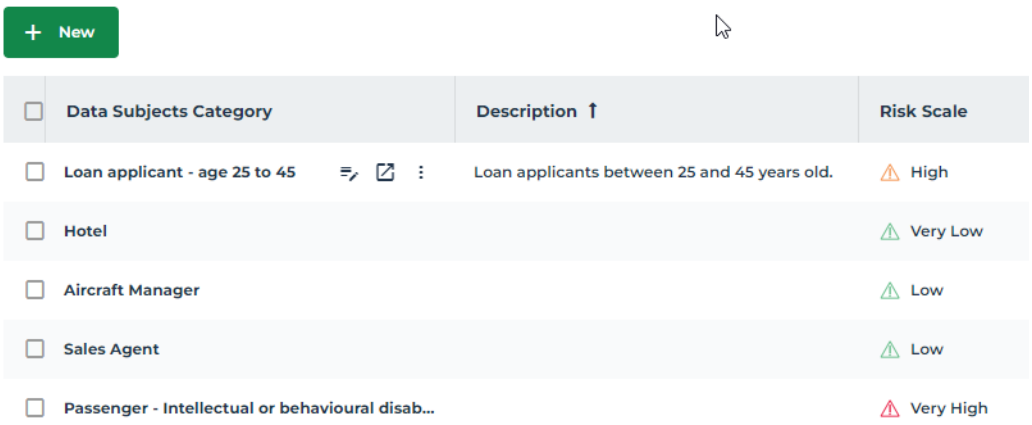
  ☛ *The risk is considered from the data subject point of view. It refers to what might occurs if data is lost, stolen or becomes unavailable.*

DATA SUBJECT CATEGORIES

A Data Subject category is a type of stakeholder which interacts with your organization in the context of the enterprise architecture environment, such as private sector customer, a supplier.

To define data subject categories:

1. Select **Key elements > Data Subject Categories.**
2. Identify all the data subject categories involved in the company processing activities (eg. employees, clients, leads, etc.).
3. Modify the default **Risk Scale** if necessary.

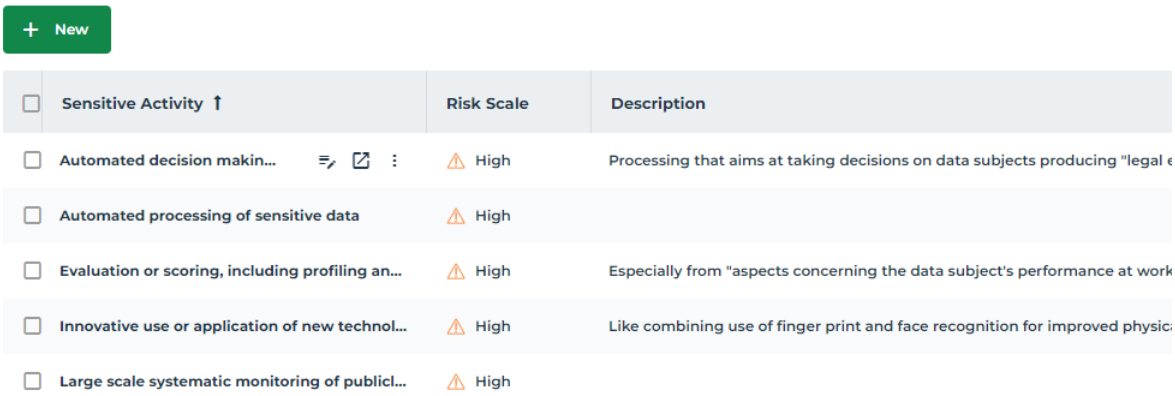


DEFINING SENSITIVE ACTIVITIES

📖 *A sensitive activity is an activity whose impact on the overall processing risk is important.*

To define sensitive activities:

- Select **Key elements > Sensitive activities.**



Hopex Privacy Management provides a pre-defined set of sensitive activities that you can edit according to your own needs, for example:

- Automated processing of sensitive data
- Large-scale processing operations of sensitive data

  ☛ *The WP29 recommends that the following factors need to be considered when determining whether the processing is carried out on a large scale:*

  - *the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;*
  - *the volume of data and/or the range of different data items being processed;*
  - *the duration, or permanence, of the data processing activity;*
  - *the geographical extent of the processing activity.*
  - *Large-scale systematic monitoring of publicly accessible areas.*
- Profiling

  ☛ *Profiling consists of any automated processing of personal data intended to evaluate, analyze, or predict data subject behavior.*

The **Risk Scale** of the sensitive activities provided by default is "High".

DEFINING TRANSFER SAFEGUARDS

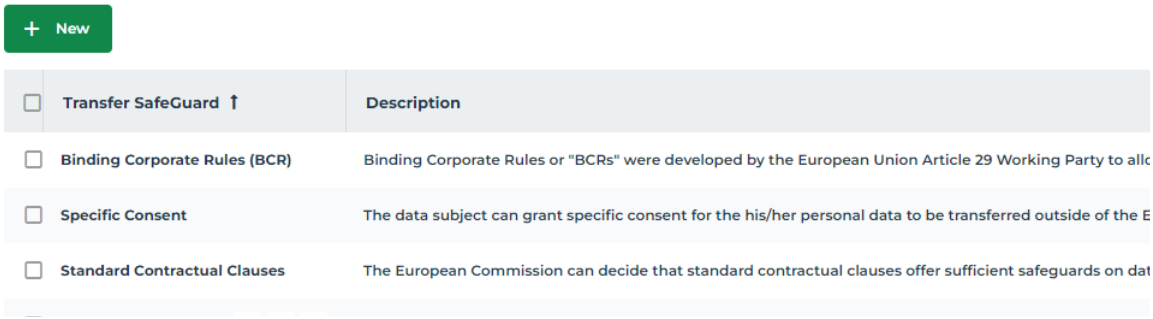
You need to make sure that transfer of personal data is legitimate and lawful.

Data transfers outside the EU are considered unlawful by default. However there may be derogations if transfer safeguards are applied.

> 🕮 *Safeguards are measures taken to ensure the legitimacy of data flows. They apply to transfers only.*

To define transfer safeguards:

- Select **Key elements > Transfer safeguards.**



The most common transfer safeguards are as follows:

- Binding Corporate Rules (BCRs): internal code of conduct adopted by multinationals to allow transfers between different branches of the organization (useful for intra-group data transfers).
- Standard Contractual clauses (SCCs)
- Specific consent

For each safeguard, you can indicate the **Mitigation** level (by default, "Very High").

DEFINING SUPERVISORY AUTHORITIES

A Supervisory Authority is a public authority which is established by a member state. It may be contacted by the legal entity for example to notify a data breach or to gather feedback on a processing activity DPIA. It makes sure that the data protection law is being applied. It may request documentation or evidence.

To access supervisory authorities:

- Select **Key elements > Supervisory Authorities.**

The objective of this section is to provide the contact data for each European supervisory authority the organization might have to contact, for example to notify a data breach, to gather feedback on a processing activity DPIA, etc.

This list is pre-populated and you can enrich it with other supervisory authorities if necessary.

The following information is provided for each supervisory authority:

- **Email**
- **Country**
- **URL**: web site address

DEFINING COUNTRY ADEQUACY

About Country adequacy

The European Union distinguishes between three types of countries:

Country	Legislation	Requirement
EU	GDPR	No safeguard needed
Outside EU	Data protection law equivalent to the GDPR	No safeguard needed
Outside EU	No data protection law	***Safeguards must be applied***

☛ *For more information on safeguards, see Defining Transfer Safeguards.*

Accessing country-adequacy information

To access country-adequacy information:

- Select **Key elements > Country GDPR adequacy.**

This section lists countries and provides information regarding the level of adequacy of the country's data protection law. The information is provided by the European Commission and is periodically updated.

Country-adequacy information use

When you describe an existing data transfer in the processing activity property page, the risk level associated to the transfer is automatically computed based on the country adequacy level.

☛ *For more information on data flows, see Specifying data transfers on a processing activity.*

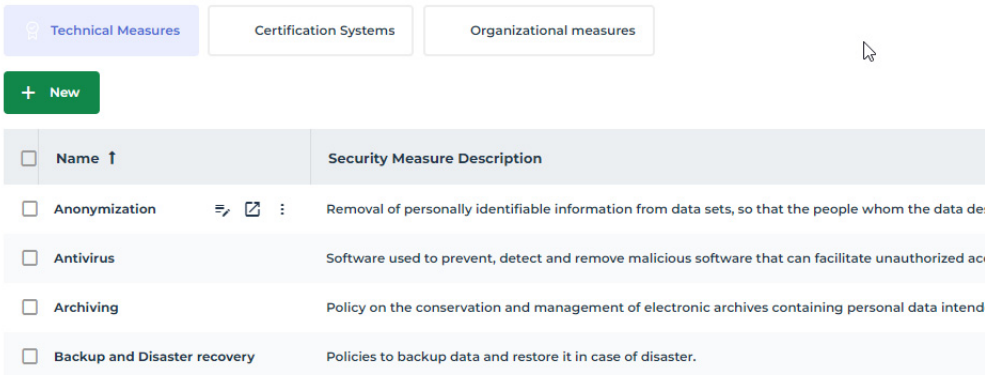
Moreover, this information may guide you when it comes to identify the transfers requiring the adoption of specific safeguards (eg. Binding corporate rules, standard contractual clauses, consent).

DEFINING SECURITY MEASURES

Under the GDPR, both data controllers and data processors must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

To access and define security measures:

- Select click **Key elements > Security Measures.**



Security measures may be of the following types:

- **Technical measures**

  Examples: Data partitioning, disaster recovery, anti-virus, Firewall

- **Organizational measures**

  Examples: Policies and procedures, assignment of specific roles, Hardware maintenance

- **Certification Systems**

  Example: ISO 27001, ISO 27018

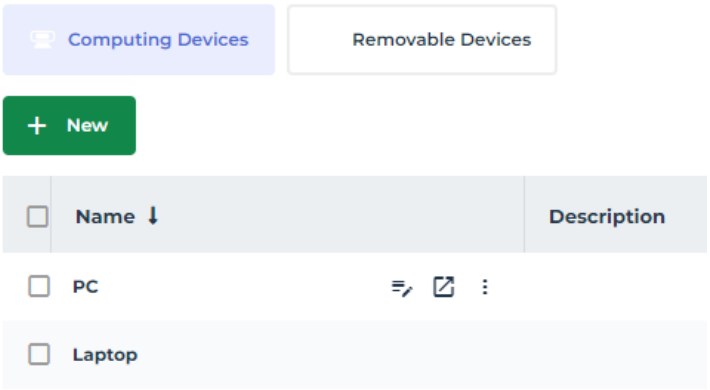
  ☛ *Security measures apply to data processing. Security measures which apply to transfers are called safeguards. For more details, see Defining Transfer Safeguards.*

DEFINING TECHNOLOGIES

To manage technologies:

- Select **Key Elements > Technologies**.

You can add computing devices or removable devices.



Computing devices

Computing devices are hardware pieces that can host and run software. Together with their hosted applications, they provide Information and IS services.

Examples: Laptop, PC, iPad.

Removable devices

This list enables you to detail removable devices used in a processing activity.

Examples: optical media (DVD), USB drive.

DEFINING PHYSICAL ARCHIVES

A physical archive corresponds to the premises in which historical records are located.

To detail physical archives:

- Select **Key Elements > Physical Archives**.

Description of physical archives includes:

- Country
- Address

DEFINING THE ORGANIZATION

As a ***Chief Privacy Officer***, you need to define the organization for the Privacy team members to be able to perform their duties.

> ☛ *Note that you can reuse EA org-units to create your privacy organization. See Converting HOPEX EA Org-Units to Organizations.*

You need to create:

- legal entities
- departments

  > ☛ *See Creating Legal Entities and Departments.*
  >
  > ☛ *It is mandatory to create entities and departments. If you do not, you will not be able to create processing activities.*

You may create:

- third parties

  > ☛ *See Managing Third Parties.*
- company guidelines

  > ☛ *See Managing Policy Documents.*
- the DPO organigram

  > ☛ *See Viewing the DPO Organizational Chart.*

CREATING LEGAL ENTITIES AND DEPARTMENTS

☛ *It is mandatory to create entities and departments. If you fail to do so, you will not be able to create processing activities.*

Introduction to Entities and Departments

A Legal Entity is a company or an organization which has legal rights and obligations.

In **Hopex Privacy Management**, an "HQ Entity" is created by default. It represents the headquarters entity in the event you have several entities in your repository.

You can create other legal entities (which cannot be considered as headquarters as there is only one default HQ entity).

☛ *For general information on entities, see Defining Legal Entity Properties.*

You need to create departments which you have to link to legal entities.

☛ *For general information on departments, see Managing Departments.*

Creating a Legal Entity

You may need to create legal entities other than the HQ legal entity.

To create a legal entity:

1. Select **Organization > Legal entities & DPOs**.
2. Click **New** to create a legal entity.

☛ *A legal entity is named an "organization" at the time of creation. Technically speaking, legal entities, establishments and departments are of the "organization" object type.*

☛ *For more information on entities, see Defining Legal Entity Properties.*

Creating Departments

To create a department:

1. Select **Organization > Departments.**
2. Click **New** and in the window that appears select a **Legal Entity**.

☛ *It is necessary to specify the legal entity managing the department being created.*

Populating Legal Entities and Departments

After creating legal entities and departments, you need to populate them with users. This enables you to grant the proper access and visibility rights.

Also, you need to be associated to a department to be able to create a processing activity.

To do so, see

- Defining Legal Entity Properties
- Managing Departments

DEFINING LEGAL ENTITY PROPERTIES

To specify information on an entity:

1. Select **Organization > Legal entities & DPOs**.
2. Select an entity.

General Properties of Entities

Indication about the **Status** of the entity can be found on the top right-hand side:

- "Live": the entity has been created or validated by the DPO / Privacy team
- "Candidate": someone without the proper rights created the entity; it needs to be validated by the DPO or Privacy team
- "Obsolete": the entity no longer exists

> ☛ *The Status is available for all main **Hopex Privacy Management** concepts.*

The property page offers more opportunities to describe legal entities.

- **Legal Entity**
- **Acronym**
- **DPO**: who the DPO is for the legal entity
- **Reporting to DPO**: who the main DPO is within a hierarchy of DPOs.

  > ☛ *It is important to fill in this field on entities to be able to display the organizational charts of DPOs. For more information, see Viewing the DPO Organizational Chart.*

- **Group HQ**: indicates whether the legal entity represents the headquarters (read-only).

  > ☛ *Only the legal entity created by default is considered as headquarters.*

- **EU Entity**: indicates whether the legal entity is located in the European Union or not (read-only).

Managing Establishments

> 🕮 *An establishment corresponds to the location (site) of a legal entity.*

For more information, see Defining Establishments.

Managing National Representatives

> 🕮 *A National Representative is a representative of the legal entity in one of the Member States. Typically, a non-European legal entity should appoint national representatives in all European Member States where*

there are data subjects whose personal data is processed by the legal entity.

Consequently, national representatives must be appointed when:

- the legal entity headquarters are based outside the European Union, and
- the legal entity processes personal data of people in the European Union.

If this is not the case, no national representatives are required.

The national representative acts on behalf of the controller or processor with regard to their obligations under privacy regulations.

To specify national representatives for an entity:

- In the entity property page, select the **National representatives** tab.

For each representative you may specify:

- the **EU coverage**: what part of Europe the national representative covers (for example All EU countries)
- the **Last audit date**: when the national representative was last audited by the legal entity.

Managing Contractual Agreements

To specify contractual agreements applicable to an entity:

- In the entity property page, select the **Contractual agreements** tab.

This section displays the list of existing contractual agreements that the legal entity signed with third parties.

A contractual agreement can be specified within the context of a Processing activity when a third party is involved. For more information, see Managing Third Parties.

The following information can be provided on a contractual agreement:

- **Contract name**
- **Reference ID**: can be defined from another tool (SAP for instance)
- **Contract scope**: enables you to specify which legal entities and departments are covered by the contract
- **Expiration Date**
- **Data Protection clauses**: enables you to specify whether the contract contains data protection specific clauses
- **Subcontracting**: enables you to indicate whether the contract authorizes the third party to sub-contract its services.
- **File**
- **Access path**

Managing Users

To assign users to a legal entity:

1. Select **Organization > Legal entities and DPOs.**

2. In the properties of a legal entity, select the **Users** tab and add the relevant users.

This section enables you to connect users who should access the information related to the current legal entity, for example its processing activities.

The users assigned have read/write permissions on objects associated to the legal entity. See also: Managing Processing Activity Visibility.

☛ *If no specific users are listed, everyone will be able to view all the processing activities of the legal entity.*

MANAGING DEPARTMENTS

☛ *To create a department, see Creating Departments.*

To access departments in **Hopex Privacy Management**:

- Select **Organization > Departments**.

In the property pages of a department, you can:

- specify general characteristics
  ☛ *See Defining department main characteristics.*
- specify the different roles played within the department
  ☛ *See Defining Department roles.*
- define the DPO and deputy DPO, which enables to display automatically an organizational chart for DPOs.
  ☛ *For more information, see Viewing the DPO Organizational Chart.*
- manage users
  ☛ *See Connecting Users to a department.*

Defining department main characteristics

The following information can be provided:

- **Department name**
- **Legal entity** associated
  ☛ *It is mandatory to specify a legal entity on a department.*

Defining Department roles

- **Department manager**
- **Deputy DPO**: person appointed by the DPO to monitor the department
- **IT support correspondent**: person providing IT support.

Connecting Users to a department

You need to add users so that processing activity owners could create processing activities.

To connect users to a department:

1. In the properties of a department, select the **Users** tab.
2. Connect the relevant users.

DEFINING ESTABLISHMENTS

An establishment corresponds to the location (site) of a legal entity.

You can describe establishments in the entity property pages.

Creating an establishment

To create an establishment:

1. Select **Organization > Legal entities and DPOs.**
2. In the properties of a legal entity, select the **Establishments** tab.

You can specify the following information for an establishment:

- **Name** of the establishment
- **Country**
- **Transfer safeguards**

  Transfer safeguards are measures taken to ensure the legitimacy of data flows towards the establishment.

  ☛ *For more information see Defining Transfer Safeguards.*
- **Certifications** if applicable

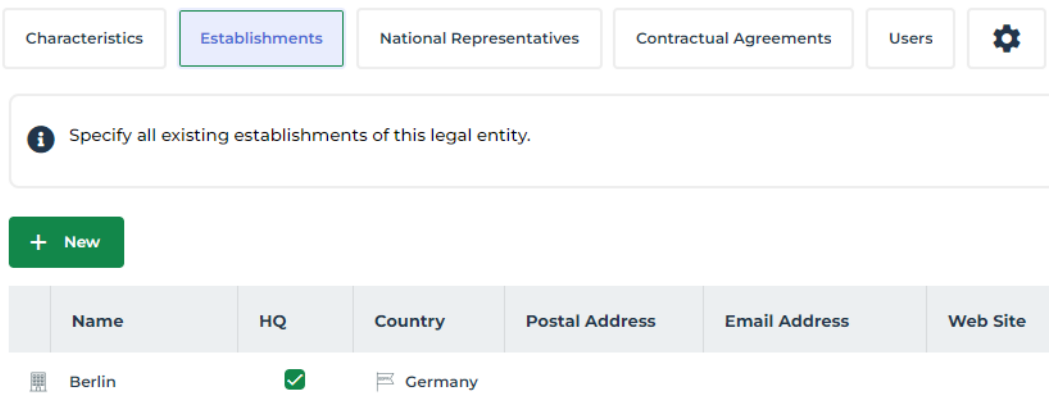
  For more information, see Specifying security measures on a processing activity

Specifying the HQ establishment for an entity

When you create several establishments, you need to define which of them represents the headquarters.

To specify the HQ establishment:

1. Select **Organization > Legal Entities and DPOs**.
2. In the legal entity property page, select the **Establishments** tab.
3. Select the **HQ** check box.



Specifying the country of a legal entity

You can specify the country on the main (HQ) establishment of the legal entity.

To specify the country of a legal entity:

1. Open the property pages of the legal entity and select the **Establishments** tab.
2. Specify a **Country** for the establishment which was declared "HQ".

> ☛ *It is important to associate a legal entity with a country to illustrate transfers. For more information on transfers, see:*
>
> - *Specifying data transfers on a processing activity*
> - *Cross-border Transfer Map*

DEFINING AN ORGANIZATIONAL MODEL

An organizational model tree enables you to define the structure under legal entities. It also enables you to specify the data protection roles involved (functions).

Defining the organizational model is usually the first step in a privacy compliance project.

To define your organizational model:

1. Select **Organization > Organizational Model**.
2. From the pop-up menu of an existing legal entity, select **Structure** and one of the following sub-menu:
   - **New Legal Entity**
   - **New Department**
   - **New Function**

Functions enable to identify different data protection roles.

- Business Responsible
- Data Controller

  A data controller is the entity that determines the purposes, conditions and means of the processing of personal data.
- Data Processor

  A Data Processor is the entity that processes data on behalf of the Data Controller.
- Data Protection Officer

  The Data Protection Officer (DPO) is an expert on data Privacy who ensures that an entity is adhering to the policies and procedures set forth in the data privacy law.
- Deputy DPO

  A deputy DPO may assist the DPO in large organizations.
- IT Support Correspondent

  An IT support correspondent is in charge of providing IT support.
- Joint Controller

  Joint controllers can work jointly to determine the purposes and means of a processing activity.

MANAGING THIRD PARTIES

Third-party management enables you to legitimate data transfers outside the European Union.

> 🕮 *A Third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.*

To manage third parties in **Hopex Privacy Management**:

- Select **Organization > Third Parties Management**.

In this section you can record all third-parties somehow involved in the processing of personal data.

> ☛ *The same information as found on legal entities can be specified here. For more information, see Defining Legal Entity Properties.*

Centralizing third party data makes it easier to control whom the personal data is shared with and if appropriate safeguards, like specific contractual clauses, codes of conducts, etc., have been implemented to ensure the lawfulness of the data transfer.

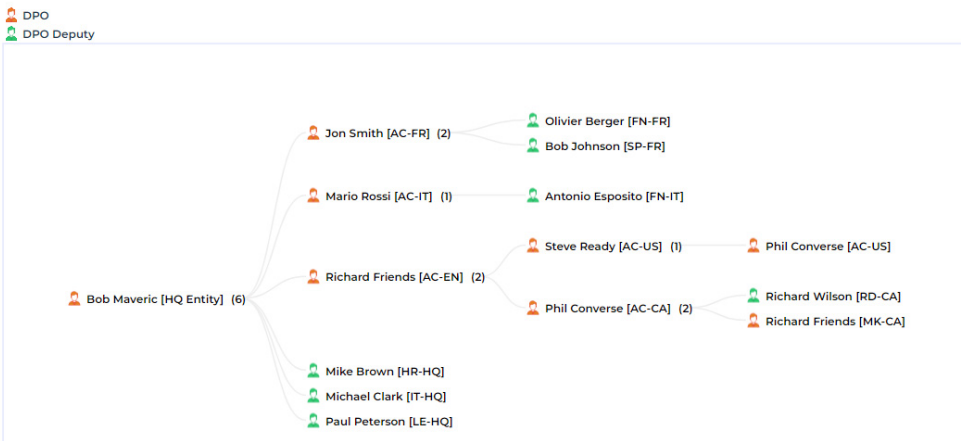
VIEWING THE DPO ORGANIZATIONAL CHART

In **Hopex Privacy Management**, the DPO organizational chart shows the DPOs hierarchy of the organization and defines who is reporting to whom in the organization.

This helps escalating problems and quickly identify the responsible person when dealing with compliance matters.

To access the DPO organizational chart:

- Select **Organization > DPO Organigram Report**.



To define a DPO organigram report if it is not already available:

1. Select **Legal Entities & DPOs**.
2. Select a legal entity and in its property page, fill in the following fields:
   - **DPO**
   - **Reporting to DPO**: enables you to specify dependencies and populate the DPO organizational chart accordingly.

MANAGING POLICY DOCUMENTS

Policy documents enable you to attach documents or specify a URL concerning privacy-relevant information the organization might use to give evidence of the company accountability.

Creating Policy Documents

To create policy documents:

1. Select **Organization > Policies & Procedures**.

You may provide the following information when creating a policy document:

- **Document name**
- **Scope**: legal entity or department concerned
- **Status:**
  - Existing: the document is available
  - Foreseen: it has been considered to provide a policy but it is not available yet
  - Not addressed: no document is available
  - Ongoing: the document is being written
- **Tag**: you can associate a tag to the policy so as to be able to retrieve it easily.

For more information on tags, see Collaboration features.

Attaching Policy Document Information

To attach the document which is important from a privacy perspective:

1. Expand the **Attachments** section of the policy document created.
2. Attach a **Business document** or create an **External Reference** indicating the relevant URL.

Assessing Policy Documents

From the list of policy documents you can specify information about the policy document assessment:

- **Review Date**
- **By**: who performed the review
- **Compliance**: the reviewer indicates how effective the document is in relation to the privacy requirements

MANAGING REGULATIONS

Hopex Privacy Management enables you to:

- ✓ define regulation frameworks and requirements

  📖 *A regulation framework is a set of directives, compulsory or not, defined by a governement in a law, by standard bodies as 'best practices' or as an internal policy in an organization.*

  📖 *A requirement is a need or expectation explicitly expressed, imposed as a constraint to be respected within the context of a regulation framework.*
- ✓ connect those regulation frameworks and requirements to processing activities.
- ✓ view the impact of regulations on processing activities

  ☛ *See also Viewing Impact of Regulations on Processing Activities.*

MANAGING REGULATION FRAMEWORKS

📖 *A regulation framework is a set of directives, compulsory or not, defined by a governement in a law, by standard bodies as 'best practices' or as an internal policy in an organization.*

Accessing Regulation Frameworks

To access regulation frameworks:

- Select **Regulations**.

A tree lists regulation frameworks, from which you can access requirements and sub-requirements.

Specifying the Scope of a Regulation Framework

You can specify the scope of a regulation framework by connecting a ***processing activity*** to the regulation framework.

To connect processing activities to a regulation framework:

1. Select **Regulations**.
2. Open the property page of a regulation framework.
3. In the **Scope** section, connect a processing activity.

In doing so, you will be able to view the regulation framework in a processing activity property page (in the form of a tree in the **Regulations** page). For more information, see Viewing Impact of Regulations on Processing Activities.

☛ *If requirements are connected to the regulation framework, these will also appear in the above mentioned tree.*

Defining Regulation Characteristics

In the regulation framework property page, you can defin a number of characteristics:

- Code
- Name
- Application Begin Date
- Application End Date
- Detailed Description

You can also:

- define **Responsibilities** according to the RACI assignment matrix model.

  ☛ *RACI is an acronym derived from the four key responsibilities most typically used:*

  - Responsible,
  - Accountable,
  - Consulted,
  - Informed
- add **Attachments**

Specifying Requirements on a regulation framework

A regulation framework consists of one or serveral requirements.

🕮 *A requirement is a need or expectation explicitly expressed, imposed as a constraint to be respected within the context of a regulation framework.*

To add requirements:

1. In the regulation framework property page, expand the **Requirements** section.
2. Create or add requirements.

   ☛ *The requirements added to the regulation framework will appear in the **Regulations** tree of the processing activity property page (if the requirement or regulation framework is connected to a processing activity). The attached requirements will also appear. For more information, see Viewing Impact of Regulations on Processing Activities.*

MANAGING REQUIREMENTS

For each regulation framework, you need to specify one or several requirements.

> 🕮 *A requirement is a need or expectation explicitly expressed, imposed as a constraint to be respected within the context of a regulation framework.*

Accessing Requirements

To access requirements:

1. Select **Regulations**.
   A tree lists regulation frameworks.
2. Expand the regulation framework folders to view the attached requirements..

Adding Requirements

To do add first-level requirements:

1. In a regulation framework property page, expand the **Requirements** section.
2. Connect existing requirements or create new ones.

To do add second-level requirements:

1. In a regulation framework property page, expand the **Requirements** section.
2. Open the property pages of the requirement of interest and expand the **Sub-Requirements** section.
3. Connect existing requirements or create new ones.

Specifying the Scope of a Requirement

The scope of a requirement consists of one or several processing activities.

To specify the scope of a requirement:

1. See Accessing Requirements.
2. In the property page of a requirement, expand the **Scope** section and connect a processing activity.

In doing so, you will be able to view the requirement in a tree in the processing activity property page (**Regulations** tab). The parent regulation of the requirement will also appear. For more information, see Viewing Impact of Regulations on Processing Activities.

Defining Requirement Characteristics

To define requirement characteristics:

1. In the requirement property page, specify the following:
   - **Code**: enables uniqu:e identification of the requirement.
   - **Parent requirement**: requirement to which this requirement is attached.
   - **Requirement type**

     A requirement type defines a standardized requirement typology within the context of an organization.
   - **Regulation framework**: regulation to which the requirement is attached.
   - **Priority** (Low, Medium, High)
   - **Issuer**: requirement-issuing organizaton

DESCRIBING PROCESSING ACTIVITIES

The processing activity is the core of **Hopex Privacy Management**. It enables the organization to describe for what purpose personal data is used and how it is managed.

As a ***processing activity owner***, you are in charge of the detailed description of a processing activity.

☛ *For information on assessment by the DPO once the processing activities have been described, see Assessing Processing Activities.*

☛ *For troubleshooting, see About Processing Activities.*

Pre-requisites to Processing Activity Creation

Your functional administration must have already created the proper organization for you to perform process activity description. The following need to be performed beforehand:

- Define legal entities
- Define departments
- Assign Users to legal entities and departments

For more information, see Defining the Organization.

CREATING PROCESSING ACTIVITIES

You can directly create processing activities in **Hopex Privacy Management**.

☛ *See Creating Processing Activities in Hopex Privacy Management.*

You can also create processing activities:

- by duplicating an existing processing activity

☛ *See Creating Processing Activities through Duplication.*

- by reusing EA processes and applications.

☛ *See Creating Processing Activities from EA Objects.*

Creating Processing Activities in Hopex Privacy Management

To create a processing activity directly in **Hopex Privacy Management**:

1. Select **ROPA**.
2. Click **New**.

If needed, you can create processing elements. If this is the case, it is advised to describe the general processing activity first then create processing elements if differences need to be specified.

☛ *For more information, see Managing Processing Activity Elements.*

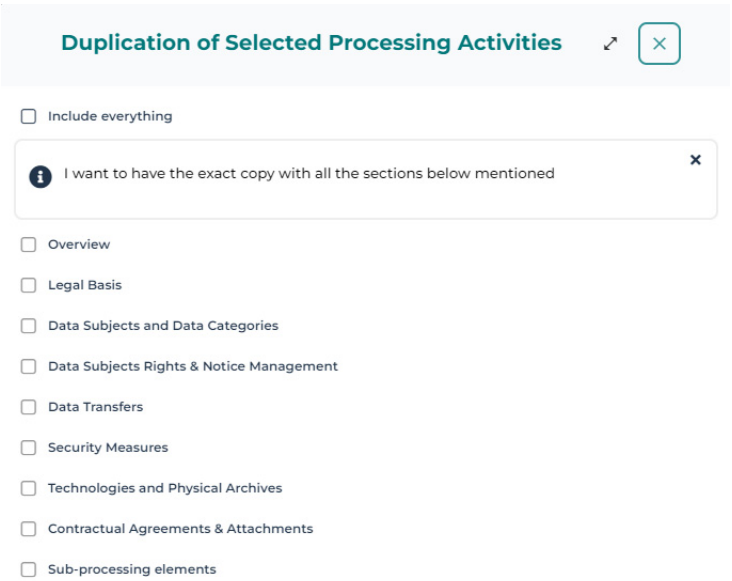
Creating Processing Activities through Duplication

You can create processing activities by duplicating an existing processing activity. The existing processing activity serves as a template.

To duplicate a processing activity:

1. Select **ROPA**.
2. Select a processing activity.
3. Click the ⋮ button that appears and select **Duplicate**.

4. In the wizard that appears, select the sections you need to duplicate:
   - Overview
     ☛ *See Processing Activities Overview.*
   - Legal Basis
     ☛ *See Processing Activities Legal Basis.*
   - Data Subjects and Data Categories
   - Data Subject Rights and Notice Management
     ☛ *See Data Subject Right and Notice Management.*
   - Data Transfers
     ☛ *See Data Transfers.*
   - Security Measures
     ☛ *See Security Measures.*
   - Technologies and Physical Archives
     ☛ *See Technologies and Physical Archives.*
   - Sub-processing Elements
     ☛ *See Managing Processing Activity Elements.*



5. Click **OK**.

ACCESSING THE RECORDS OF PROCESSING

Accessing Processing Activities

To access processing activities in **Hopex Privacy Management**:

1. Select **ROPA**.
2. Select a processing activity to open its property page.

If you have a lot of processing activities in your record of processing, you can refine the scope of the processing activities you wish to display. See Refining the Scope of the Records of Processing.

Refining the Scope of the Records of Processing

Data privacy laws may require you to produce two separate records of processing activities:

- one as data controller
- one as data processor

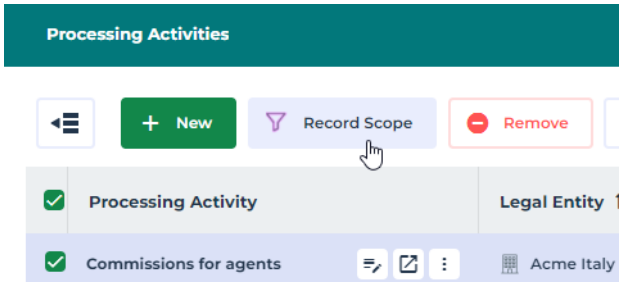
Hopex Privacy Management includes an advanced filter to quickly export the record of processing of one or more entities based on their protection role.

To refine the scope of the processing activities displayed in your record of processing:

1. Access the record of processing.

   ☛ *See Accessing Processing Activities.*

2. In the list of processing activities click the **Record Scope** button at the top of the list.



3. Specify the **Legal Entities** you are interested in.
4. Specify the data protection role played:
   - **Data Controller**
   - **Joint Controller**
   - **Data Processor**
5. Click **Apply**.

The list of processing activities is updated as a function of the criteria specified.

Describing Processing Activities

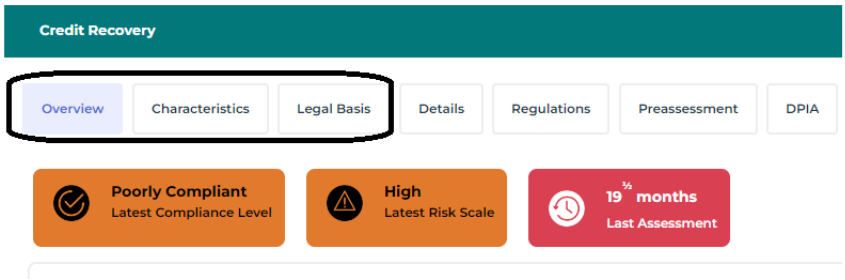
DESCRIBING PROCESSING ACTIVITIES

☛ *For more information about processing activity creation, see Creating Processing Activities.*

☛ *See also Accessing Processing Activities.*

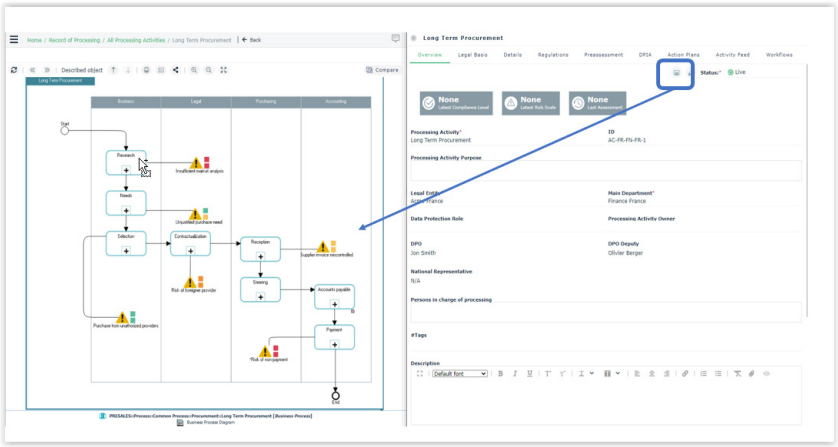
As a processing activity owner, you need the first three tabs in the processing activity property page to fully describe processing activities:

- **Overview**: see Processing Activities Overview.
- **Legal Basis**: see Processing Activities Legal Basis.
- **Details**: see Processing Activity Details.



☛ *The **Pre-assessment** and **DPIA** tabs are to be used by the Privacy team only. For more information, see Assessing Processing Activities.*

Note that a processing activity which originates from a HOPEX process displays an icon representing the process next to the status of the processing activity:

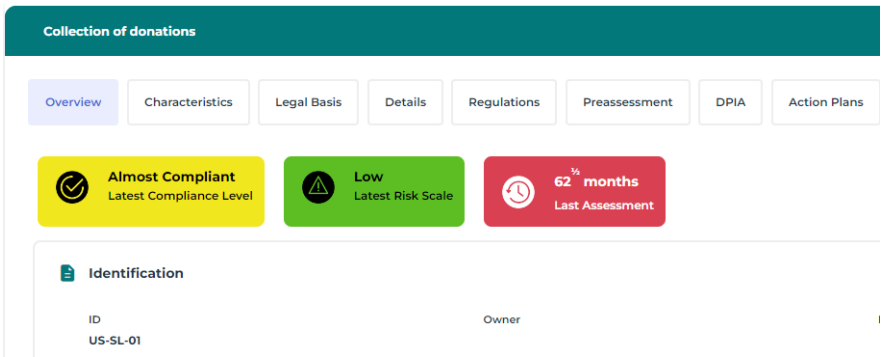


Processing Activity Dashboard

At the top of the page, you are given an overview of the processing activity.

The information displayed here takes into account the assessments made through pre-assessments and DPIAs. This dashboard is empty until the Privacy team starts to assess the processing activity.

☛ *For more information, see Consulting DPIA Reports and Results.*



Describing Processing Activities

Processing Activities Overview

Additional information to specify

The property page of a processing activity displays general information about the processing activity:

- **Processing Activity** Name
- **ID**: identifier

  ☛ *The identifier is automatically computed based on the acronyms of the associated legal entity and department.*
- **Processing Activity Purpose**: enables you to enter free text to describe the purpose of the processing activity

  🕮 *The purpose of a processing activity is the main objective of this processing activity. Examples: satisfaction survey, customer management, site monitoring.*
- **Data Protection Role**: enables you to specify the role played by the legal entity
  - "Data Controller"

    🕮 *A data controller is the entity that determines the purposes, conditions and means of the processing of personal data.*

    ☛ *It is mandatory to specify a data controller.*
  - "Data Processor"

    🕮 *A Data Processor is the entity that processes data on behalf of the Data Controller.*
  - "Joint Controller"

    🕮 *Joint controllers are data controllers who jointly determine the purposes and means of a processing activity.*
- **Processing Activity Owner**

  🕮 *The processing activity owner provides a detailed description of the processing activity (excluding assessment).*
- **Description**: enter a comment
- **Sensitive activities**: specify any particular operation carried out in the context of this processing activity that could impact the final risk level.

  ☛ *For more information, see Defining Sensitive Activities.*
- **Start Date** and **End Date**
- **IT Processing / Paper Processing**: specify whether the processing activity uses automated or paper means or both
- **Persons in charge of processing**: enter manually the actual people in charge

Information in read-only mode

Some fields are automatically filled in (they are in read-only mode only):

- **Legal Entity**
- **Department**
- **DPO**

  ☛ *The DPO is defined at the legal entity level.*

- **DPO deputy**

  ☛ *The DPO deputy is defined at the department level.*

- **National representative**

  🕮 *A National Representative is a representative of the legal entity in one of the Member States. Typically, a non-European legal entity should appoint national representatives in all European Member States where there are data subjects whose personal data is processed by the legal entity.*

  ☛ *This field provides information on the level of coverage of the European countries. For more information, see Managing National Representatives.*

  - "Full": all representatives for all EU countries have been assigned.
  - "Partial": at least one national representative covering at least one EU country has been assigned.
  - "No": no representative has been assigned so far
  - "N/A": the legal entity is located in the EU; it is not necessary to specify national representatives.

Participants involved in the processing activity

You can specify which other participants are allowed to take part in the processing activity.

To specify additional participants:

1. In the processing activity property page, unfold the **Other participants** section at the bottom of the page.
2. Connect:
   - **Legal Entities**
   - **Departments**

     ☛ *Note that by default the following entities and departments are automatically granted access:*

     - *The legal entity and the main department defined in the processing activity Overview page.*
     - *All legal entities appearing in the processing activity Details page, under the Processing Element table.*

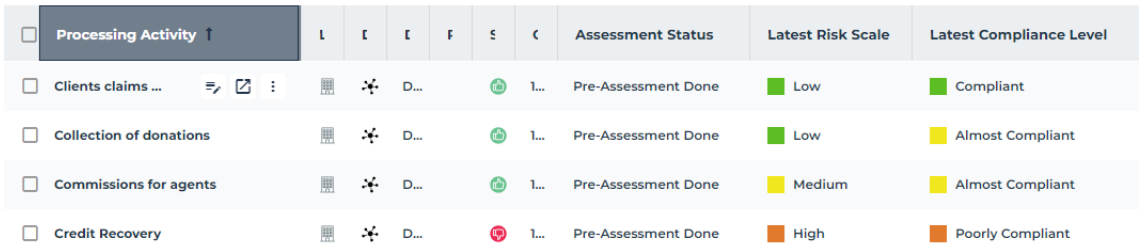
Describing Processing Activities

Computed information

The columns of the list of processing activities display computed information based on assessments (whether pre-assessments or DPIAs) such as:

- the **Assessment status**: indicates whether an assessment has be performed or not
- **Latest risk scale**
- **Latest compliance level**

☛ *If no assessments have been performed, the cells remain empty.*

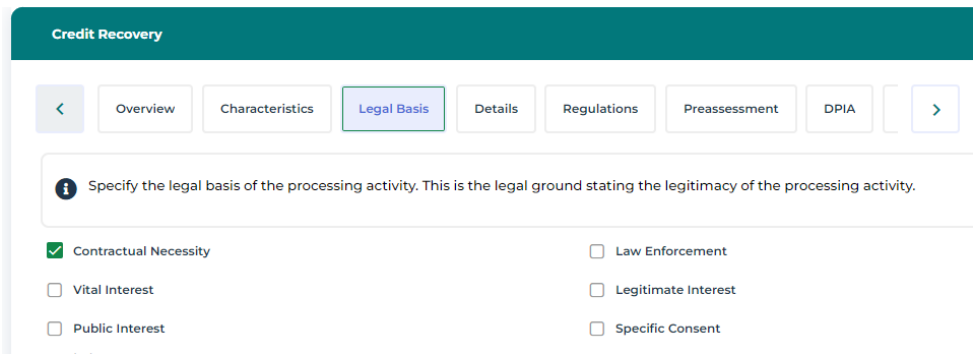


Processing Activities Legal Basis

You need to specify the legal basis of the processing activity and provide as attachment any relevant document. This is the legal ground stating the legitimacy of the processing activity.

To specify the legal basis:

❱ In the processing activity properties, select the **Legal Basis** page.



You must have a valid lawful basis in order to process personal data.

🕮 *The legal basis is what gives you permission to carry out the processing activities.*

There are different lawful bases for a processing activity. In the GDPR, these are set out in Article 6. At least one of these must apply when you process personal data.

- **Specific consent**: the data subject has freely given clear consent for you to process his/her personal data for a specific purpose.

  📖 *Consent is a freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.*

  Example: processing of personal data for email marketing

- **Contractual necessity**: the processing is necessary due to the fulfillment of a contract

  Example: processing of employees data for payroll management

- **Law enforcement**: the processing is necessary for you to comply with the law (this does not include contractual obligations).

  Example: Bank processing of clients data to prevent money-laundering

- **Vital interest**: the processing is necessary to save or protect an individual's life.

  Example: processing of patients data for medical treatment

- **Public**: the processing is necessary for you to perform a task of public interest or within your official functions (the task or function having a clear legal basis).

  Example: processing of personal data related to potential criminal convictions or offences for investigation purposes

- **Legitimate interests** the processing activity is strictly connected to the service provided by the business mission. The business could not exist without this processing activity.

  Example: processing of visitors personal data for security reasons

  ☛ *If you select **Legitimate interest** as a legal basis, it may be useful to provide additional information in the comment field provided. This legal basis generally requires detailed evidence to justify the legitimacy of the processing activity.*

The Privacy team can later assess the **Legal basis** based on the check boxes previously selected by the processing activity owner.

PROCESSING ACTIVITY DETAILS

The processing activity **Details** page represents the core of the processing activity description.

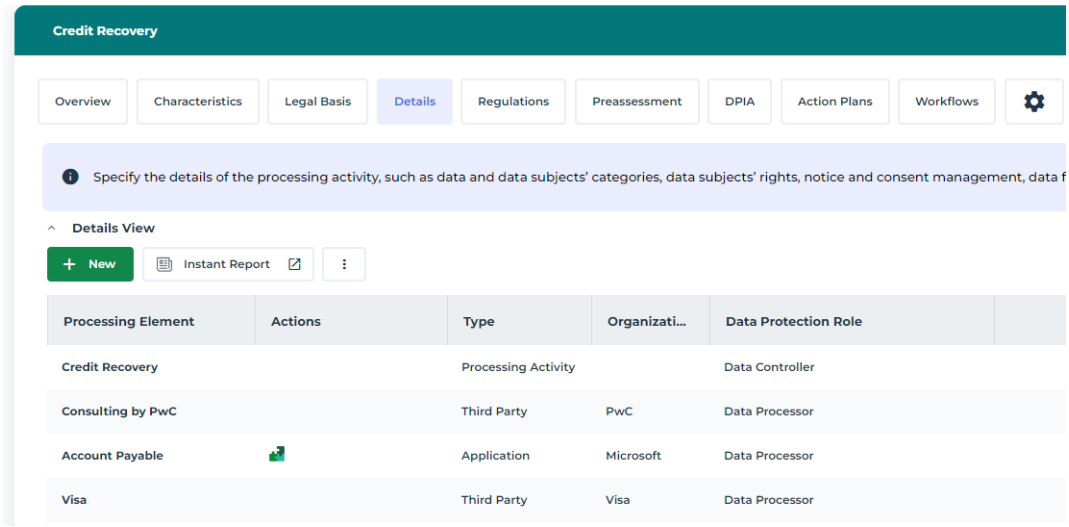
Processing Activities Levels of Detail

Every processing activity needs to be described at a general level. Yet, it may be useful to create processing elements if you use an IT application or a third-party to process your activity.

You therefore need to:

- start by describing the processing activity at a general level
- (optional) create processing elements and enter the information which differs from that entered on the general processing activity.

  ☛ *For more information, see Creating a processing element.*



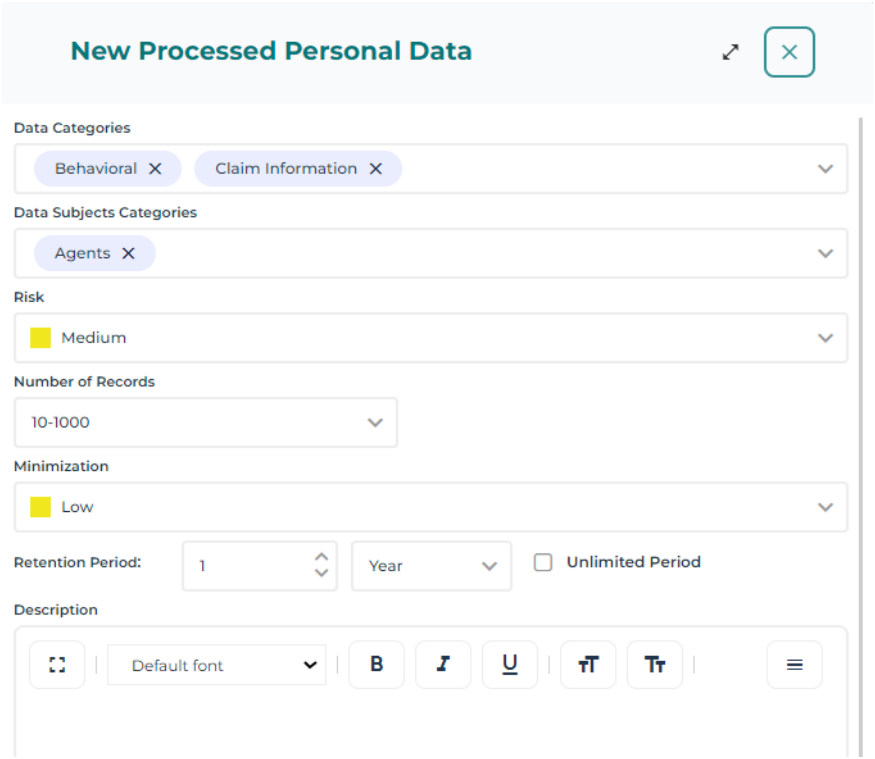
For the general processing activity you can enter the following information:

- Processed Personal Data
- Data Subject Right and Notice Management
- Data Transfers and Security Measures
- Technologies and Physical Archives
- Contractual Agreements and Other Attachments

Processed Personal Data

To create processed personal data in **Hopex Privacy Management**:

1. Open the processing activity properties.
2. In the **Details > Processed Personal Data** section, click **New**.



In this window you can specify the following information:

- **Data categories**
- **Data subjects categories**
- **Number of records**: corresponds to the number of data subjects in your records of processing.
- **Minimization**

  Minimization is a principle stating that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

  ☛ *see Qualifying Minimization*
- **Retention period**

  ☛ *see Specifying the retention period on a processing activity*

Qualifying Minimization

Minimization is an important principle of the European Union's General Data Protection Regulation (GDPR) and other data protection laws.

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for with they are processed. Additionally, data collected for one purpose cannot be re-purposed without further consent.

Possible minimization values	Meaning
Low/Very low	Too much information is used
High	The information used is strictly what is needed

The Privacy team can later give a compliance score for the Personal Data Risk section based on the information completed by the processing activity owner:

- Select a value from the **Data Mininization Compliance Level** drop-down menu.

Viewing the computed risk

On creation of the processed personal data, the **Risk** is automatically computed based on the highest risk scale specified by the functional administrator in the **Key elements** section (for the concerned data categories and data subject categories).

A risk represents any risk related to data privacy that should be identified and assessed during a DPIA process.

For more information on the initial risk scales filled in by the functional administrator, see Defining Data Categories and Data Subject Categories.

Specifying the retention period on a processing activity

Specifying a retention period on your processing activity is essential. The actual retention period may be determined by local laws.

After specifying the actual retention period, the goal retention period is compared to the actual one. The color of the icon indicates how compliant you are with your initial goal.

The goal retention period corresponds to the lowest default retention period of the selected data categories.

Data Subject Right and Notice Management

This section is available from the **Details** tab of the processing activity property page.

In this section you can specify the following:

- the data subjects' rights granted by this processing activity.

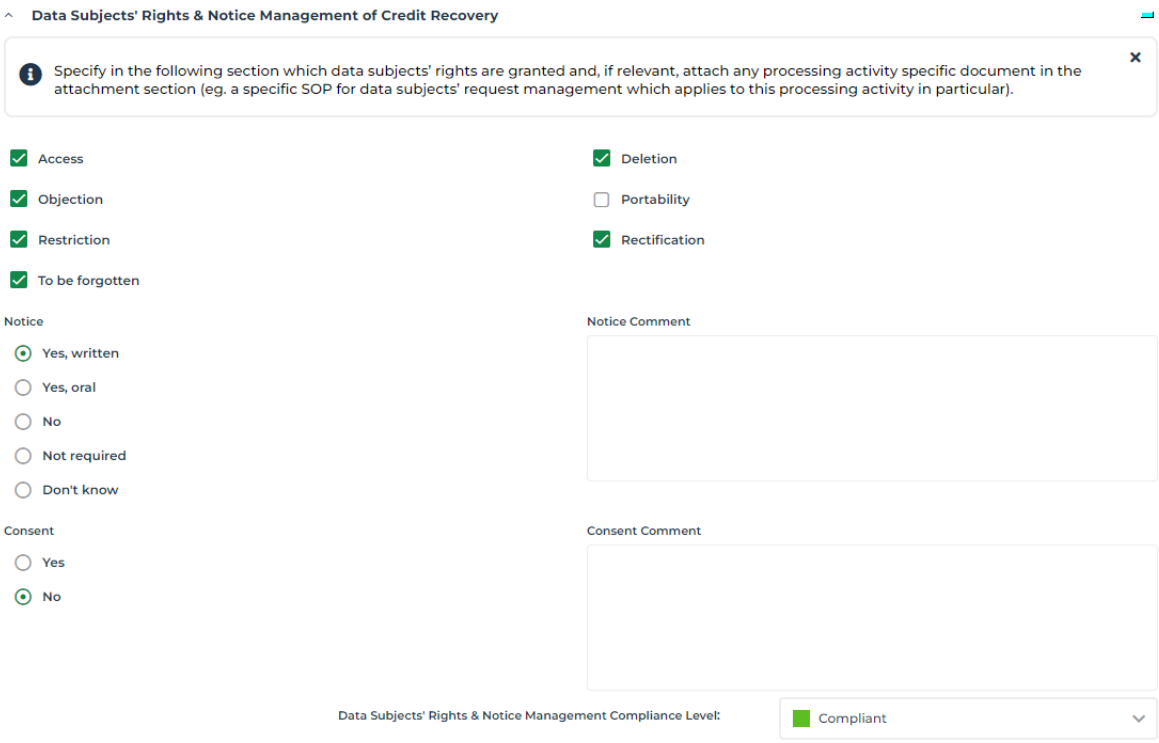
  ☛ *See Specifying data subject rights for a processing activity for more information.*

- how the notice is managed (in writing, orally, not required)

  ☛ *To view a notice management report of all processing activities, see NoticeThird-Parties.*

- whether specific consent is collected or not

  🕮 *Consent is a freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.*



Specifying data subject rights for a processing activity

You can specify the rights that have been taken into account in your processing activity.

☛ *A least one data subject right must be selected here.*

- **Access**

  🕮 *Right to Access entitles the data subject to have access to and information about the personal data that a controller has concerning them.*

- **Object**

  ☛ *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her*

- **Restriction**

  ☛ *The data subject shall have the right to obtain from the controller restriction of processing.*

- **To be forgotten**

  🕮 *The Right to be forgotten is also known as Data erasure. it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.*

- **Deletion**

  🕮 *A data subject may also have the right to have you delete data that you keep on him or her.*

- **Portability**

  🕮 *Data Portability is the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.*

- **Rectification**

  ☛ *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.*

Viewing data subject rights for all your processing activities

As an activity or application owner, you may want to view the data subject rights of the processing activities you are responsible for.

Hopex Privacy Management provides a report for this.

To have a general view of the data subject rights:

❱ In the processing activity owner desktop, click **Reports > Data Subjects' rights**.

Giving a compliance score for data subject rights

The Privacy team can later give a global compliance score for this section based on the above mentioned information. To do so:

❱ Select a value from the **Data Subjects' rights and notice management Compliance level** drop-down menu.

Data Transfers

> 🕮 *Under a data privacy law, a data transfer is a transfer or copy of personal data.*

This section enables you to create data transfers specific to your processing activity.

To create data transfers and security measures on a processing activity:

1. Open the property page of a processing activity.
2. Select the **Details** tab.

Specifying data transfers on a processing activity

When creating a data transfer, you can specify:

- the transfer name
- the recipient (legal entities and subcontractors)

  > ☛ *The recipient country is automatically deduced from the main establishment of the entity.*
- the sender
- the data categories and data subjects involved

  > 🕮 *Data category is used to group different personal data. See Defining Data Categories for more information*

  > 🕮 *A Data Subject category is a type of stakeholder which interacts with your organization in the context of the enterprise architecture environment, such as private sector customer, a supplier. See Data Subject Categories for more information.*
- the safeguards applied

  > 🕮 *Safeguards are measures taken to ensure the legitimacy of data flows. They apply to transfers only.*
  >
  > *For more information, see Defining Transfer Safeguards.*
- whether data is outsourced
- whether data is sold/bought.

Giving a compliance score for transfers

The Privacy team can later give a global compliance score for this section based on the above mentioned information. To do so:

1. From the **Details** tab of the processing activity page, scroll down to the section corresponding to transfers.
2. Select a value from the **Data Transfers Compliance level** drop-down menu.

Security Measures

Specifying security measures on a processing activity

To create a group of security measures specifically applicable to a processing activity:

1. See Accessing Processing Activities.
2. In the property page of a processing activity, select the **Details** tab.
3. Scroll down to the **Security Measures** section and select the tab corresponding to the type of security measures:
   - Technical measures
   - Organizational measures
   - Certification systems
4. Click **New**.
5. In the **Subject** field enter a general naming for your group of security measures.
6. From the **Security Measures** drop-down list, select the individual security measures you need for your processing activity.

   ☛ *For more information on those individual security measures, see Defining Security Measures.*
7. Enter a description.
8. Select the **Mitigation level** intended through this group of security measures.

Giving a compliance score for security measures

The Privacy team can later give a global compliance score for this section based on the above mentioned information.

To do so:

1. From the **Details** tab of the processing activity page, scroll down to the section corresponding to security measures.
2. Select a value from the **Security measures Compliance level** drop-down menu.

Technologies and Physical Archives

This section enables you to connect computing/removable devices and physical archives specific to your processing activity.

To add technologies and physical archives to a processing activity:

1. Open the property page of a processing activity.
2. Select the **Details** tab and scroll to the **Technologies and Physical Archives** section.

You can connect objects of the following categories (which have been populated by the functional administrator):

- Computing device
- Removable device
- Physical archive

> ☛ *For more information, see Defining Technologies and Defining Physical Archives.*

Contractual Agreements and Other Attachments

You can connect contractual agreements or notice templates to inform a data subject for example.

> ☛ *You can find templates in the **Hopex Privacy Management** documentation from the following menu: **Record of processing > Learning material and Templates**.*

To attach a contractual agreement:

1. In the **Details** tab of a processing activity page, expand the **Contractual Agreements and Other Attachments** section.
2. Select the **Contractual Agreeements** tab.
3. Click **New**.
4. Fill in the fields as appropriate:
   - **Contract name**
   - **Contract scope**
   - **Expiration date**
   - **Privacy specific clause**: yes/no
   - **Subcontracting**: specify whether there may be sub-contractors or not for this processing activity.

MANAGING PROCESSING ACTIVITY ELEMENTS

If you need to have a global view you may want to deal with the general processing only (which means there is no need for processing elements).

For more information, see:

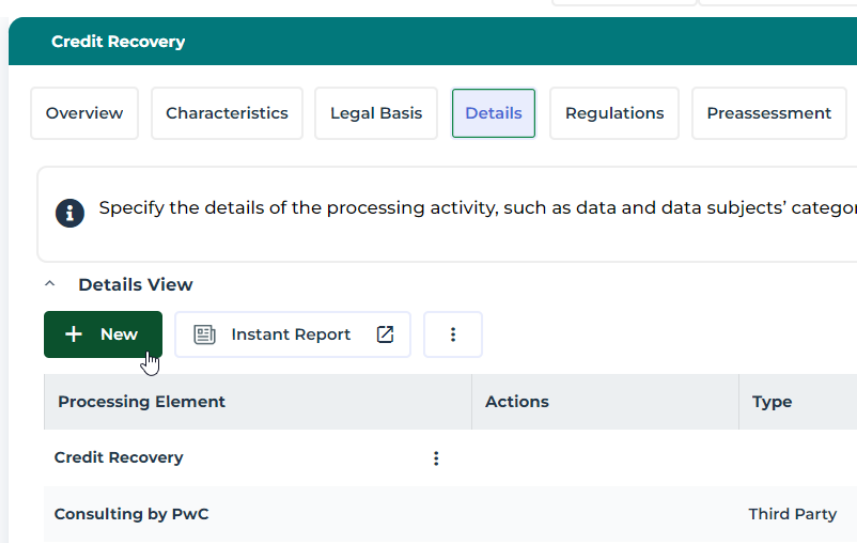
- Creating Processing Activities
- Describing Processing Activities

However if there is an IT application or a third-party involved, you may want to define processing elements in order to properly describe the processing activity.

Creating a processing element

To create a processing element:

1. Access a processing activity and open its property page.
2. Select the **Details** tab.
3. In the **Details View** section, click **New**.



4. Select a type of processing element.
   - Organization
   - Third-party
   - Application

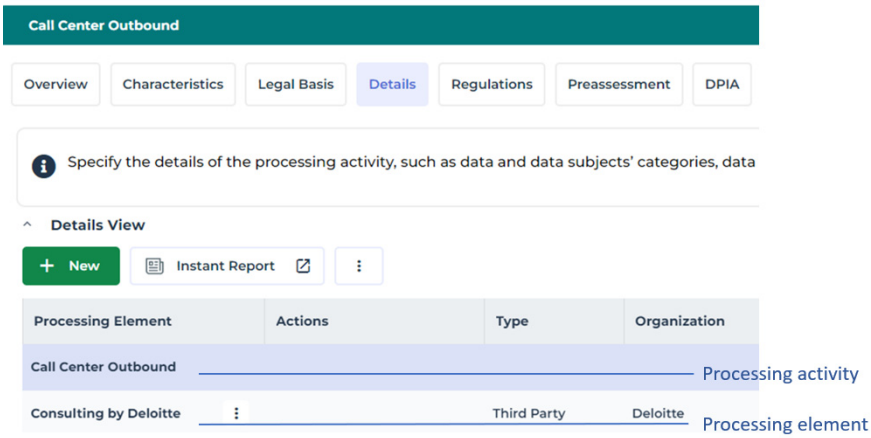
   ☛ *For more information, see Specifying an application processing element.*

You can provide information about the data protection role of the application provider or third-party.

To describe the processing element:

1. Select the processing element created.

2. Notice that from now on the property page applies to the processing element:



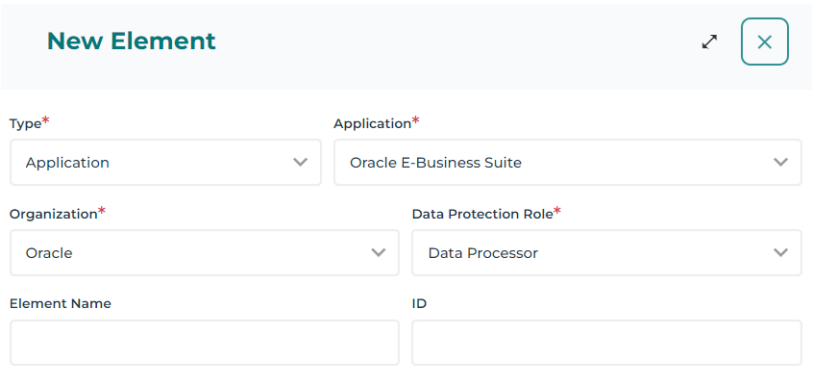
Specifying an application processing element

To specify a processing element of application type:

1. Create a processing element.

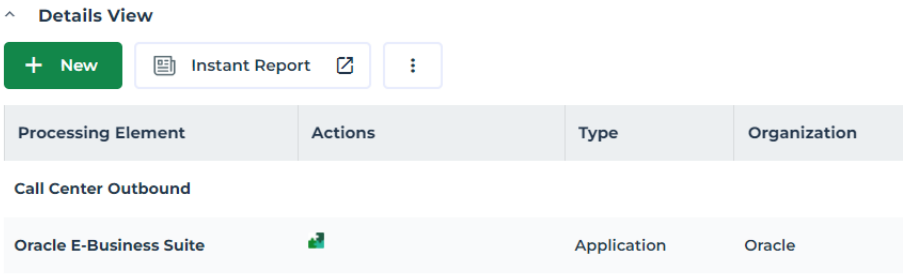
   ☛ *See Creating a processing element.*

2. In the **Type** drop-down list, select "Application".
3. If applications from other **Hopex** solutions have been imported in **Hopex Privacy Management**, select one of them in the corresponding drop-down list.



4. Click **OK**.

5. The processing element appears below the main processing activity.



Displaying the application properties and web site

The applications coming from other **Hopex** solutions such as **Hopex IT Portfolio Management** are indicated by an application icon.

A link to an external web site is available when the application is described in a statical web site.

Viewing Impact of Regulations on Processing Activities

Hopex Privacy Management enables you to view the regulations which apply to a specific processing activity.

To view applicable regulations:

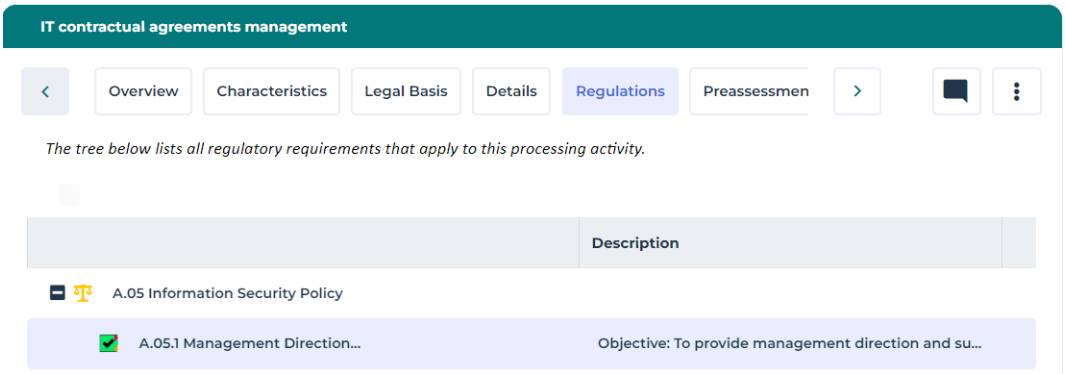
- In the processing activity property page, select the **Regulations** tab.

A navigation tree displays the regulations and requirements applicable to the processing activity. This tree is in read-only mode.

☛ *To view the tree, you must have previously and properly defined the scope (processing activities) of your regulations and requirements from the **Regulations** section.*

For more information, see:

- *Specifying the Scope of a Regulation Framework*
- *Specifying the Scope of a Requirement*



USING THE PROCESSING ACTIVITY WORKFLOW

A standard workflow enables you to manage the lifecycle of a processing activity.

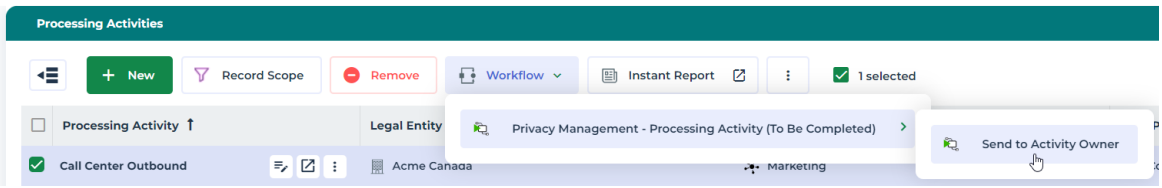
The chief privacy officer creates the processing activity. He asks the processing activity owner to complete the processing activity description. Once the processing activity has been described, the chief privacy officer can validate it. Then, pre-assessment and eventually DPIAs can be performed.

☛ *For more information on the complete workflow, see What are the possibilities offered by the standard processing activity workflow?*

Requesting processing activity description

To send the processing activity:

- Right-click the processing activity and select the following:

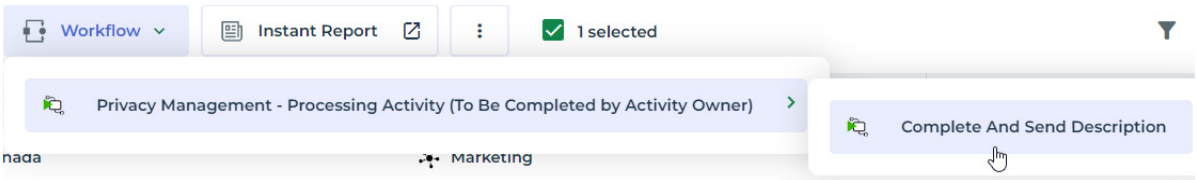


The processing activity owner can connect to **Hopex Privacy Management** with the corresponding profile and complete the description of the processing activity.

☛ *You must have previously selected a processing activity owner in the processing activity property page.*

Submitting processing activity description

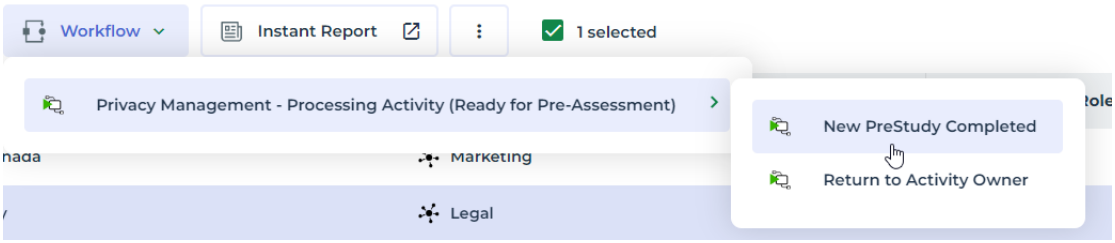
After completing the processing activity description, the processing activity owner can send it to the Privacy team. They will in be able to start pre-assessment based on what the processing activity owner specified.

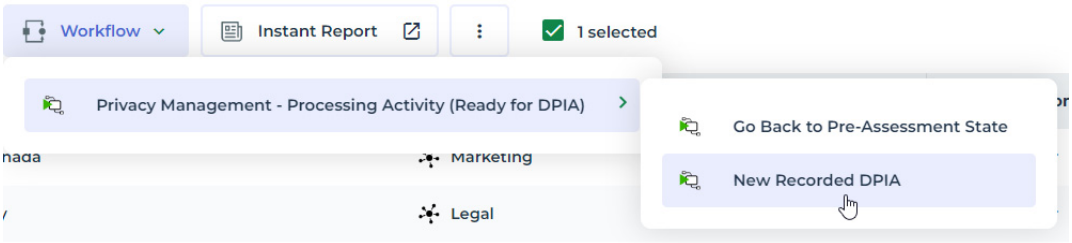


Submitting pre-assessments and DPIAs

After the activity owner has completed and submitted processing activity description, the Chief Privacy Officer can start assessments (pre-assessments and then DPIAs when needed).

☛ *If the description of the processing activity is not entirely satisfactory, a member of the Privacy team might want to return it to the processing activity owner for review.*





PROCESSING-RELATED REPORTS

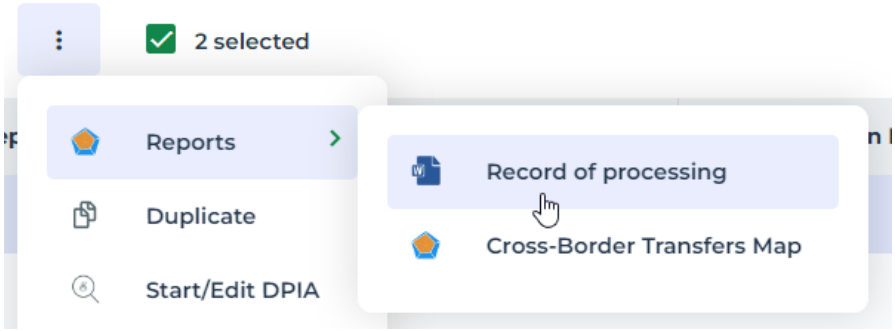
Accessing Processing-Related Reports

To generate processing activity-based reports:

1. Select a processing activity.

   ☛ *See Accessing Processing Activities.*

2. Select a report available from the **... > Reports** button drop-down menu.



Records of Processing

☛ *See Accessing Processing-Related Reports.*

About the record of processing

The information collected in the record of processing is the core of the data privacy law documentation system. It must remain available at all times in the event it is requested by the Data Protection Authority.

> 🕮 *The Data Protection Authority is a national authority tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.*

The record of processing is about ***who*** processes ***what*** personal data, ***where***, ***why***, and ***how***.

Creating a record of processing

To generate a record of processing in the form of a Word document:

1. Select **ROPA**.
2. Select a processing activity and from the **Reports** drop-down button select **Record of Processing**.

A Word document is generated. The contents is as follows:

- ***Introduction***: it describes data subject rights, the principle of data transfers and security measures.
- ***List of all processing activities***
- ***Detailed description of the processing activity selected***
  - Data protection role
    - ☛ *See Processing Activities Overview.*
  - Sensitive activities
    - ☛ *See Processing Activities Overview.*
  - Legal basis
    - ☛ *See Processing Activities Legal Basis.*
  - Data categories and Data subject categories
    - ☛ *See Processing Activities Overview.*
  - Notice and consent management
    - ☛ *See Data Subject Right and Notice Management.*
  - Data subject rights
    - ☛ *See Data Subject Right and Notice Management.*
  - Transfers to third parties
    - ☛ *See Data Transfers.*
  - Security measures
    - ☛ *See Data Transfers.*
  - Sub-processing elements
    - ☛ *See Processing Activities Overview.*
  - Attachments
    - ☛ *See Contractual Agreements and Other Attachments.*

Cross-border Transfer Map

You can generate a cross-border transfer map displaying a world map with the data transfers selected.

☛ *See Accessing Processing-Related Reports.*

Pre-requisites to using cross-border transfer map

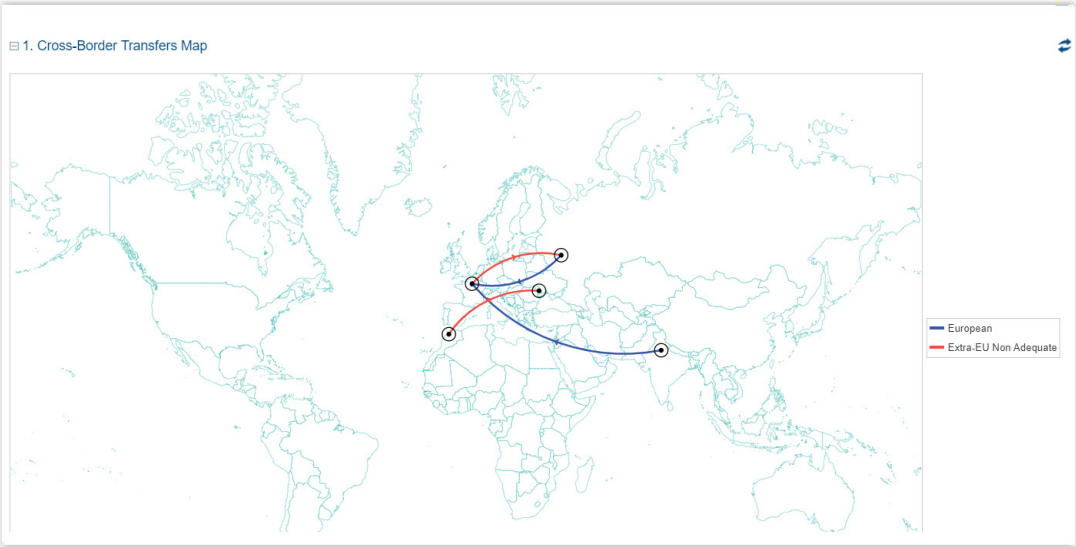
Make sure that:

- a country was specified on the HQ establishment of the legal entities involved.
  - ☛ *For more information, see Specifying the country of a legal entity.*
- you specified both a recipient and a sender on the transfer
  - ☛ *For more information, see Specifying data transfers on a processing activity*

Content of the transfer map

The country of the recipient determines whether the transfer is adequate or not.

☛ *If a transfer is non-adequate, you can source the target establishment and discover which safeguards are implemented in this establishment. For more information on safeguards, see Defining Transfer Safeguards.*



☛ *You can use the mouse wheel to zoom in or out.*

Additional information about transfers

For more information on how to create transfers, see Specifying data transfers on a processing activity.

For troubleshooting, see About Transfers.

CNIL-Specific Report

Hopex Privacy Management enables you to generate a report which conforms to CNIL requirements (French National Commission to protect personal data and preserve individual liberties).

Activating the CNIL Report

This Excel report concerning processing activities is an optional output of the record of processing. You therefore have to activate a specific option to be able to generate it.

To activate the CNIL report:

1. In the main menu, select **Settings > Options**.

2. Unfold the **Privacy** folder.
3. Select "Activate the CNIL report in the list of record of processing activities".
4. Click **OK**.

Prerequisites for the CNIL report

For the processing activities to be included in this report, you must have specified the Data Protection Role "Data controler" in their property page.

Generating the CNIL report

To generate this report:

1. Select **ROPA**.
2. Select the processing activities of interest to you (those for which the "Data Controler" data protection role has been specified).
3. from the toolbar **More** button, select **Reports > Record of Processing - CNIL format**.

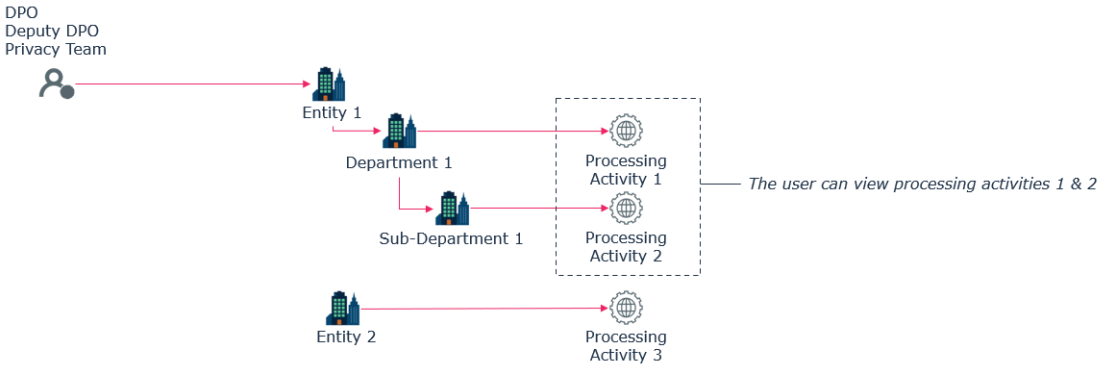
   ☛ *If no processing activities match the appropriate scope, a warning appears.*
4. Specify the **Legal entity** (data controller) who is exporting the record of processing.

   ☛ *Only the legal entities linked to the processing activities having "Data Controller" as a data protection role are suggested here.*
5. Click **OK**.

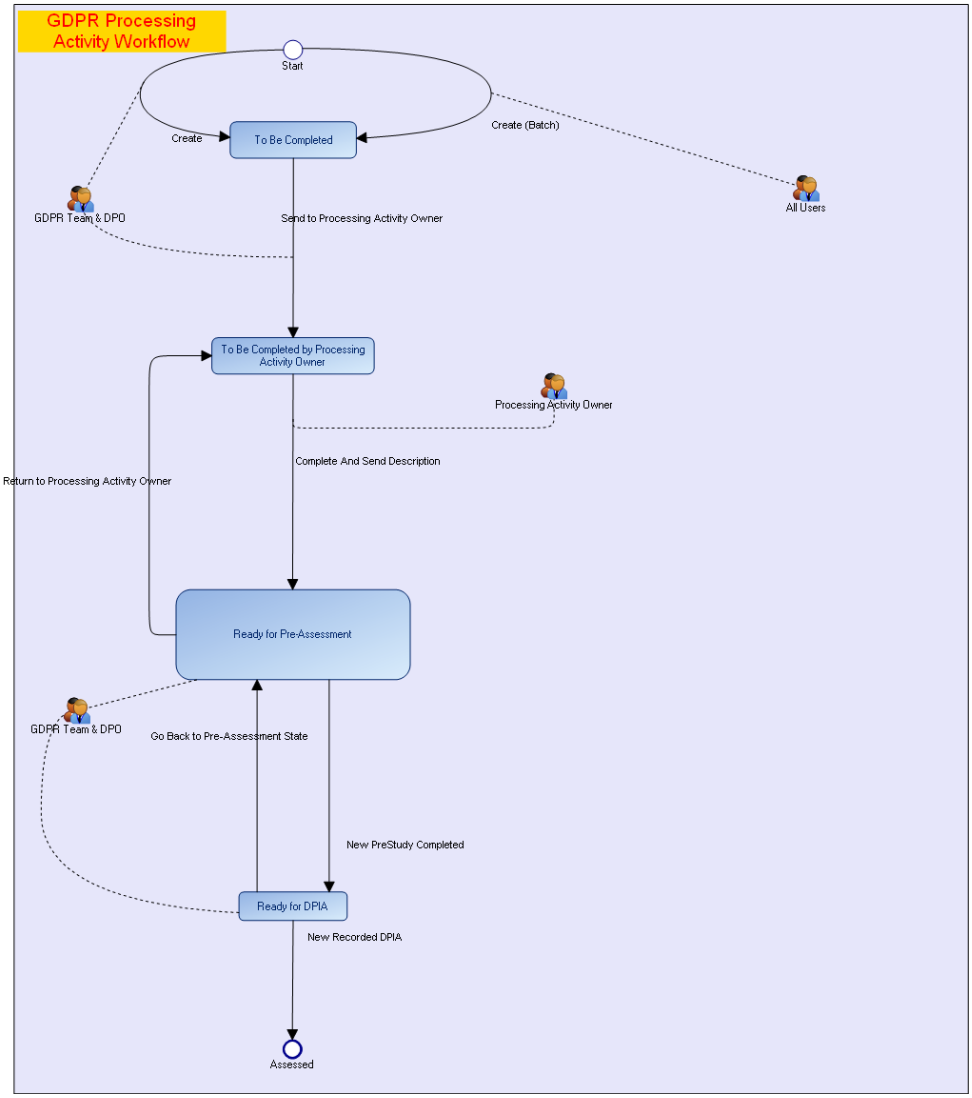
The Excel report is generated.

MANAGING PROCESSING ACTIVITY VISIBILITY

A user with a DPO, DPO Deputy or Privacy Team profile who has been assigned to a legal entity or department has access to all the processing activities associated to sub-legal entities and sub-departments.



PROCESSING ACTIVITY WORKFLOW



ASSESSING PROCESSING ACTIVITIES

Processing activities assessment is performed by the Privacy team or the DPO after the processing activities have been described by the processing activity owner.

☛ *For more details on processing activities description, see Describing Processing Activities.*

As a Privacy team member assessing processing activities, you need to use the following pages:

☛ *For assessment troubleshooting, see About Assessments.*

PREREQUISITES TO PROCESSING ACTIVITY ASSESSMENT

To be able to perform an assessment (whether a pre-assessment or a DPIA), you should make sure that:

- processing activity owners have properly described the processing activities

  ☛ *For more information, see Describing Processing Activities.*

- you have specified compliance levels on the basis of the information given by processing activity owners.

  ☛ *See Specifying Compliance Levels.*

Specifying Compliance Levels

The Privacy team/DPO has to specify a compliance level for each section of a processing activity.

☛ *It is necessary to give those scores after the processing activity owner has described the processing activity. This will give you an indication of where to start when it comes to further assessing your processing activities (through preliminary assessment and DPIAs).*

Legal Basis Compliance Level

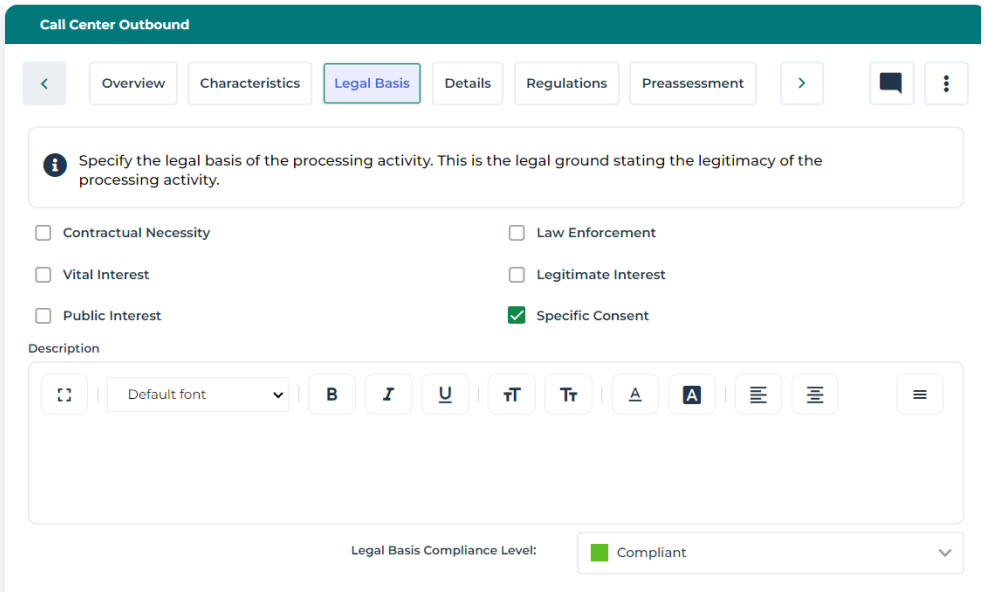
To specify a compliance level in relation to legal basis:

1. Open the processing activity property page.

   ☛ *See Accessing Processing Activities.*

2. Select the **Legal Basis** page.

3. Select a value in the drop-down menu available



There has to be at least one legal basis selected. If there is no legal basis for the processing activity, the processing activity is considered poorly compliant.

☛ *For more information see Processing Activities Legal Basis.*

Minimization Compliance Level

To specify a compliance level in relation to data minimization:

1. Open the processing activity properties.

   ☛ *See Accessing Processing Activities.*
2. Select the **Details** page.
3. Expand the **Personal Data Risk Analysis of** "your Processing Activity" section.
4. Select a value in the drop-down menu available.

   ☛ *For more information about data minimization, see Processed Personal Data.*

Data transfers and security measures

To specify a compliance level in relation to data transfers and security measures:

1. Open the processing activity properties.

   ☛ *See Accessing Processing Activities.*
2. Select the **Details** page.
3. Expand the **Security Measures** section.
4. Select a value in the drop-down menu available.

   ☛ *For more information see Data Transfers.*

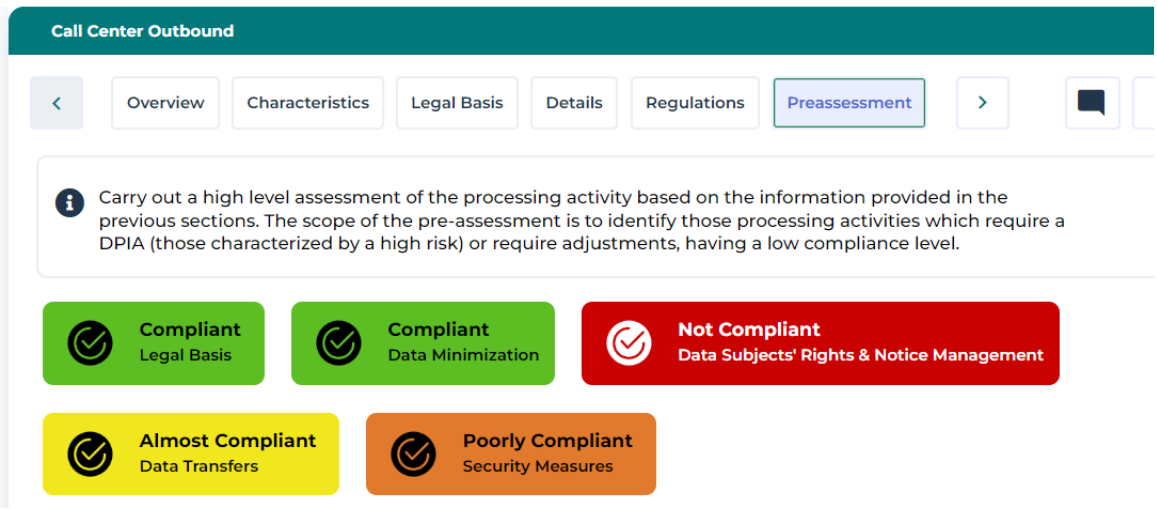
Viewing the Initial Compliance Level of a Processing Activity

It is useful for the DPO or the Privacy team to get an overview of the processing activity compliance levels. It will facilitate prioritization of subsequent actions (decide if you need to perform a pre-assessement or a DPIA).

To identify the compliance level of a processing activity:

- In the processing activity properties, select the **Pre-assessment** page.

Here you can find a summary of the scores previously assigned in the different sections found in the **Legal Basis** and **Details** pages:



- Legal Basis (score from the **Legal Basis** page)
  - ☛ *See Processing Activities Legal Basis*
- Data Minimization (score from the **Details** page)
  - ☛ *See Processed Personal Data*
- Data Subject's Rights & Notice Management (score from the **Details** page)
  - ☛ *See Data Subject Right and Notice Management*
- Data Transfers (score from the **Details** page)
  - ☛ *See Data Transfers*
- Security Measures (score from the **Details** page)
  - ☛ *See Security Measures*

PERFORMING A PRE-ASSESSMENT

The objective of pre-assessment is to identify those processing activities which have a low compliance level and require a DPIA or require adjustments.

> ☛ *Before starting your pre-assessment, we recommend to take a look at the compliance levels which were given by the processing activity owner. See Viewing the Initial Compliance Level of a Processing Activity*

Performing the Pre-Assessment

Based on the compliance scores made available in the pre-assessment dashboard, you can:

- Give a final validation score
- Define subsequent actions.

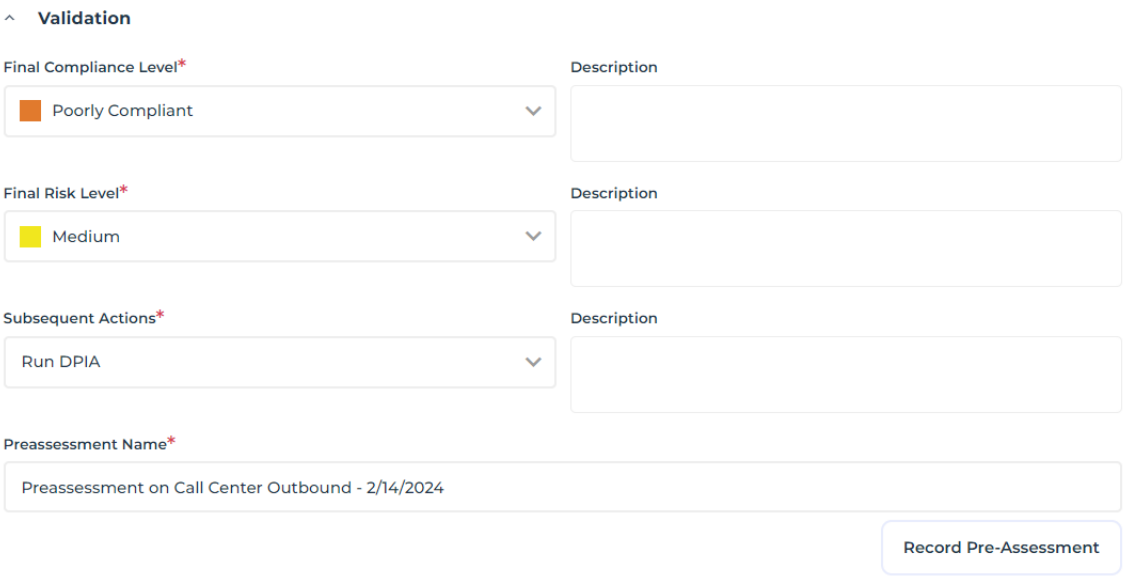
To record your pre-assessment:

1. In the **Pre-assessment** page of the processing activity properties, expand the **Validation** section.
2. Select a value for the **Final Compliance level** and the **Final Risk Level**.

   > ☛ *These fields are initialized based on the various compliance levels which have been entered beforehand.*

3. Enter a comment to justify your choice.
4. Indicate the **Subsequent Actions** to perform:
   - Nothing
   - Stop Processing Activity
   - Notify Supervisory Authority
   - Others

5. Once you have entered all the necessary information, click **Record Pre-assessment**.



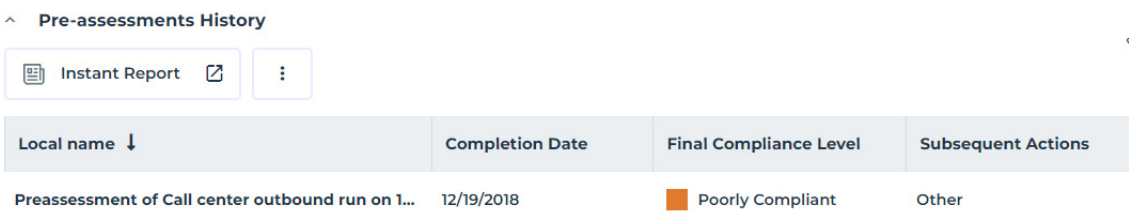
☛ *If the final compliance level is poor, you need to perform a DIPA. For more information, see Performing Impact Assessment (DPIA).*

Consulting the History of Pre-assessments

When you record the pre-assessment, it is stored in the **History** section with the data protection values which have been entered.

To access the history of pre-assessments:

- In the **Pre-assessment** page of the processing activity properties, expand the **Pre-assessment History** tab.



You can consult the property pages of the recorded pre-assessment in read-only mode.

PERFORMING IMPACT ASSESSMENT (DPIA)

About DPIAs

When to conduct a DPIA?

If the pre-assessment indicates that the risk is high, you (the DPO or the Privacy team) must conduct a DPIA.

> ☛ *For more information on pre-assessment see Performing the Pre-Assessment.*

When the processing is likely to result in a high risk to the rights and freedoms of the data subjects, a DPIA is mandatory.

What is a DPIA?

A DPIA is a detailed risk assessment.

The DPIA needs to display:

- the characteristics of the processing activity
- the risks which may have an impact on compliance.

  > ☛ *For more information, see Creating and Assessing Risks for a DPIA.*
- the remediation actions ensuring the processing activity is under control

  > ☛ *For more information, see Recommendations and Remediation Actions on DPIAs.*

Creating a DPIA

Starting a new DPIA

To start a DPIA:

1. In the property page of a processing activity, select the **DPIA** tab.
2. Click **Start DPIA**.
   In the window that appears, the risk levels identified through your pre-assessment appear.

You may also want to open an existing DPIA and edit it. See Reusing a DPIA.

Reusing a DPIA

When a processing activity shares the same risks as another processing activity, you may want to re-use an existing DPIA.

To do so, you need to import a DPIA, which consists in importing the risks and recommendations associated. This way you can reuse what you did in another DPIA. You can edit it to make it more appropriate to the current processing activity.

To import a DPIA:

1. See *Accessing Processing Activities*.
2. In the processing activity page, select the **DPIA** tab.
3. Click **Start DPIA**.
4. In the DPIA creation page which appears, click **Import DPIA**.
5. Select an existing DPIA

   ☛ *The relevant DPIA must already exists in the DPIA history.*

The data entered in the selected DPIA has been imported. You can now modify them to suit your current DPIA.

Editing a DPIA

When a DPIA has already been created and it is not finalized yet, you can modify it through the **Edit DPIA** button.

☛ *When finalized, the **Edit** button is no longer available. You need to start another DPIA. For more information see Starting a new DPIA.*

Accessing the list of DPIAs

To access all DPIAs:

❱ In the navigation bar, select **Registers > DPIAs**.

Creating and Assessing Risks for a DPIA

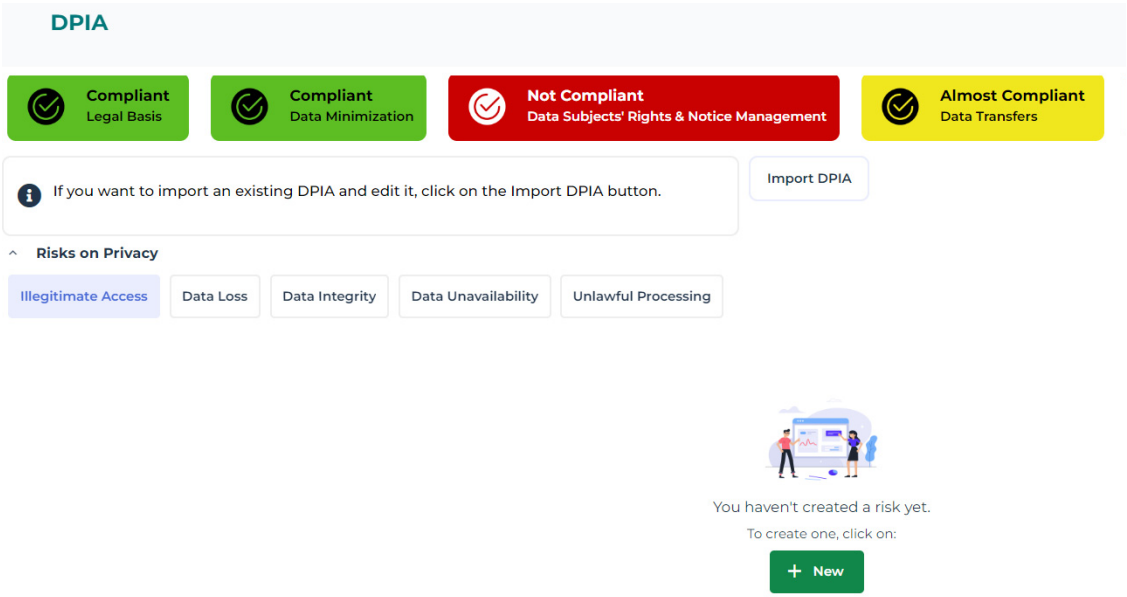
You have just started to create your DPIA.

☛ *For more information, see Creating a DPIA.*

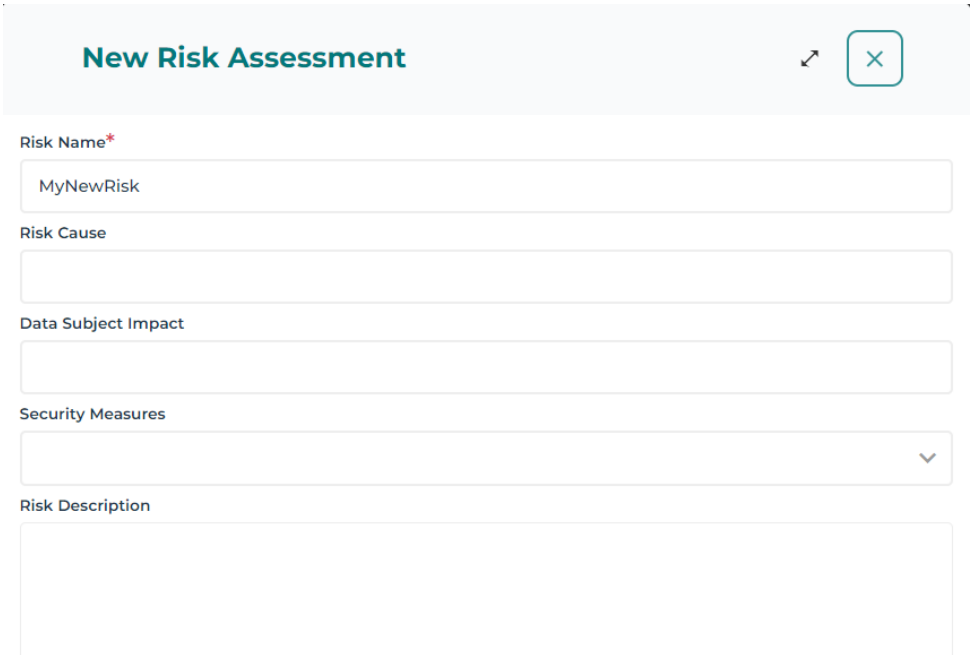
The first step when performing a DPIA consists in creating and assessing risks.

To create risks in a DPIA:

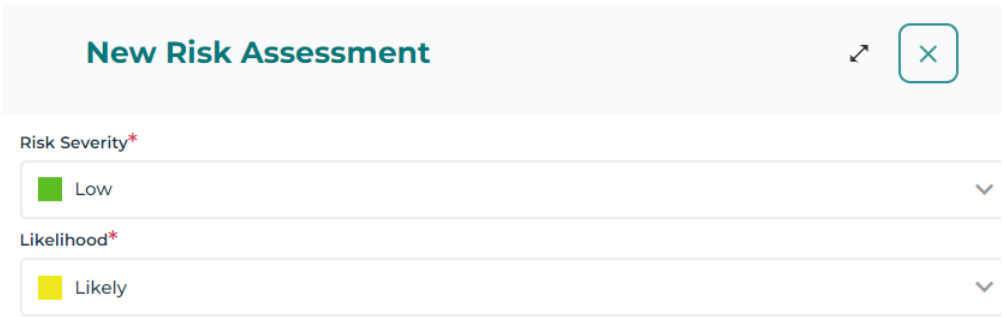
1. In the DPIA **Risks on Privacy** section, click **New** to create a risk in one of the tabs corresponding to the different risk types:
   - **Illegitimate Access**
   - **Data Loss**
   - **Data Integrity**
   - **Data Unavailability**
   - **Unlawful Processing**



2. In the first page of the wizard, enter the following:
   - **Risk Name**
   - **Risk Cause:** most common causes that could lead to a risk
   - **Data Subject Impact**: main impact on the data subject if a risk occurs
   - **Risk Description**



3. Click **Next**.
4. In the second page of the wizard, assess the risk:
   - **Risk Severity:** from "negligible" to "maximum"
   - **Likelihood**: from "rare" to "very likely"



5. Click **OK**.

Recommendations and Remediation Actions on DPIAs

When performing a DPIA you need to define

- general recommendations,
- remediation actions based on action plans.

Creating recommendations

Recommendations are based on the risk assessments previously created within the framework of the DPIA.

☛ *For more information, see:*

- *Creating a DPIA*
- *Creating and Assessing Risks for a DPIA*

To create recommendations within the framework of a DPIA:

1. In the DPIA creation wizard, expand the **Recommendations and Remediation actions** section.
2. In the **Risk Description** field, select one or several risk assessments to connect to the recommendation.
3. Provide the following information:
   - **Recommendation description**: give a comment for your recommendation
   - **Resulting risk**: specify the intended risk obtained after the remediation actions have been implemented.

Creation remediation actions

After defining general recommendations, you may decide to implement actual action plans. This will enable you to follow-up the actions taken to mitigate risks.

☛ *An action plan comprises a series of actions, its objective being to reduce risks and events that have a negative impact on company activities or to improve a process or an organization efficiency.*

For more information, see Managing Action Plans.

Validating the DPIA

Once you have created the DPIA and created risks, you can validate the DPIA.

☛ *For more information, see:*

- *Creating a DPIA*
- *Creating and Assessing Risks for a DPIA*

To validate a DPIA:

1. In the DPIA creation wizard, expand the **Validation** section.
2. Complete the following data to draw final conclusions.

Final risk level

- very low
- low
- medium
- high
- very high

Final compliance level

- Non-compliant
- Poorly compliant
- Almost compliant
- Compliant

☛ *This field is initialized based on the various compliance levels which have been entered beforehand.*

Subsequent Actions

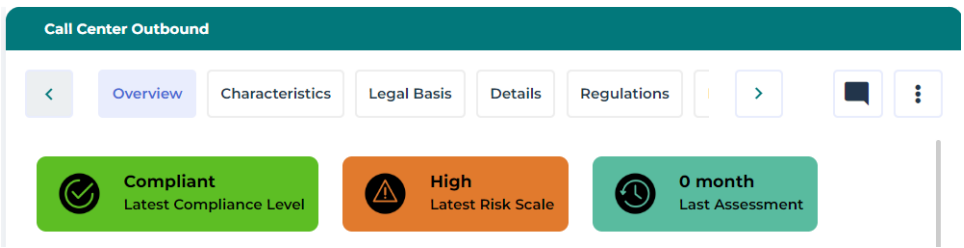
In this section you have to indicate what do next based on the different indicators obtained:

- Nothing
- Stop processing activity
- Notify supervisory authority
- Others

Consulting DPIA Reports and Results

Viewing the dashboard of the processing activity

After you performed the DPIA, the **Overview** tab of the processing activity property page displays a dashboard with updated results.



Latest compliance level and Latest risk scale

These indicators are computed based on the latest pre-assessments or DPIAs.

☛ *The most recent of the two is taken into account.*

Last assessment

This gives you an indication of when the last assessment was made (whether a pre-assessment or a DPIA).

Record of DPIAs

See Data Category and Data Subject Compliance

Generating a DPIA document

To generate a DPIA document:

1. In the **DPIA** page of the processing activity properties, expand the **DPIA History** section.
2. In the DPIA pop-up menu, select **DPIA report**.

The DPIA document executive summary contains the following information:

- The overall compliance level of the processing activity prior to the DPIA.
- A summary of the identified risks through the DPIA, with their impact and recommendations for their mitigation.
- The final risk level and compliance level obtained at the end of the risk assessment.

MANAGING DATA BREACHES

Hopex Privacy Management enables the data controller to keep a record of data breaches, as required by the law.

Hopex Privacy Management also enables to:

- assess the data breach gravity from the data subject point of view
- decides who needs to be notified based on this assessment:
  - if there is a risk associated to the breach, the supervisory authority needs to be informed
  - If the risk associated is high, the data subject needs to be informed
- identify remediation actions in the form of action plans

☛ *Those actions may be followed in other **Hopex** solutions.*

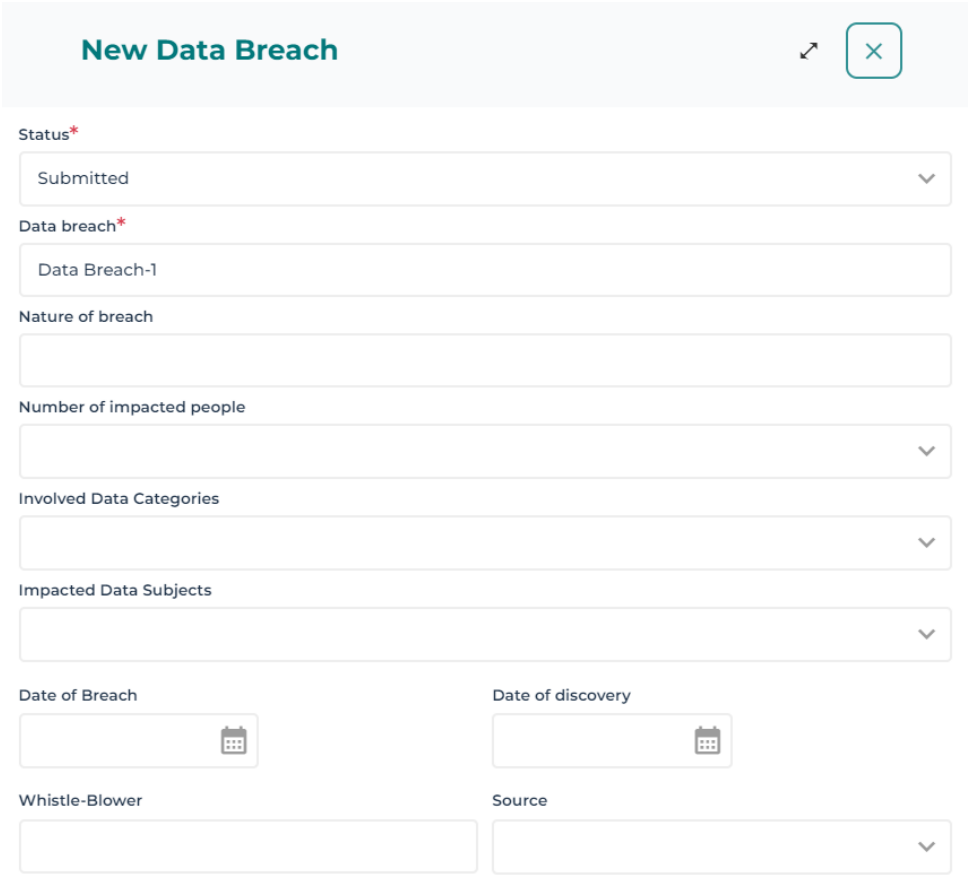
Declaring a Data Breach

Anyone can enter a data breach through **Hopex Privacy Management**.

Example of data breach: An employee accesses data he is not allowed to access.

To enter a data breach:

1. From the navigation bar, select **Registers > Data Breaches** and click **New**.



2. Describe the data breach as follows:
   - **Number of impacted people**
   - **Impacted data subjects**

     ☛ *For more information, see Data Subject Categories.*
   - **Involved data categories**

     ☛ *For more information, see Defining Data Categories.*
   - **Date of breach**
   - **Date of discovery**

     ☛ *The date of discovery is important as you only have 72 hours to collect, assess and report the data breach. See Viewing Elapsed Time since Breach Discovery.*
   - **Whistle-blower**: stakeholder who reports the incident
   - **Source**: external claim, internal control, internal alert, other

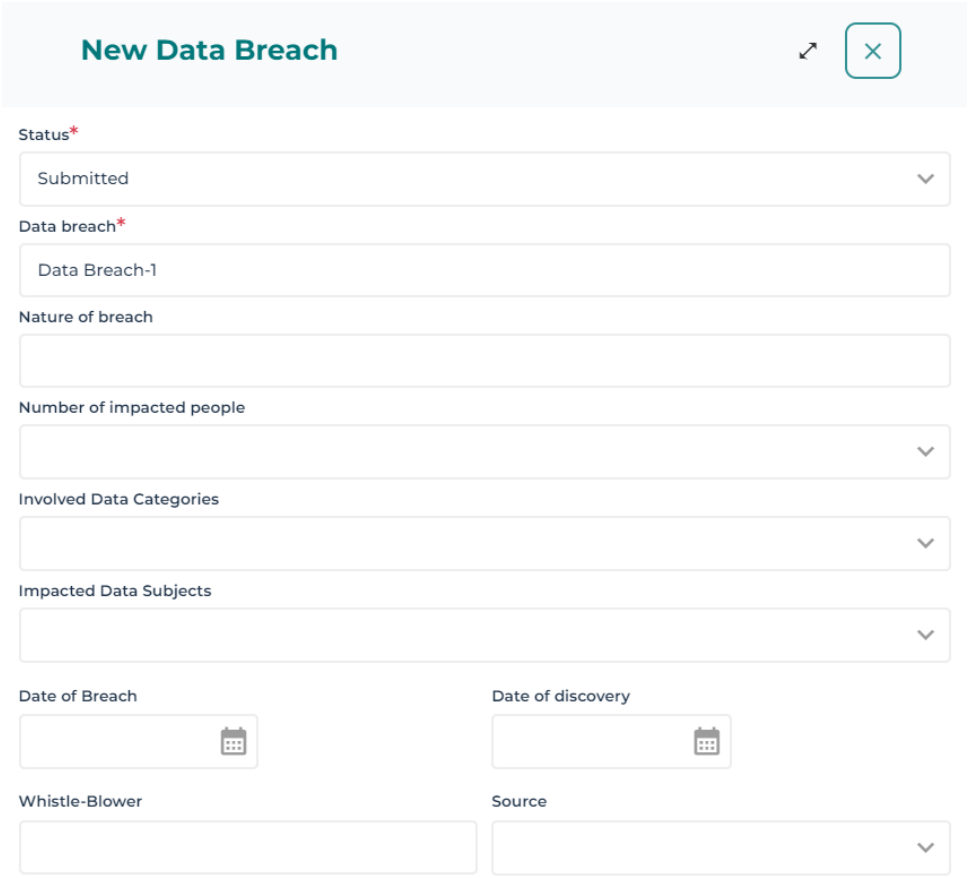
Once the data breach has been created, you can provide information related to:

- breach scope
- breach assessment: see Assessing a Data Breach
- breach notification: see Notifying a Data Breach

Specifying Data Breach Scope

You can describe the scope of the data breach, i.e. which legal entities, departments and processing activities are impacted by the breach.

The scope of the data breach also determines who can view the breach information.



Assessing a Data Breach

To assess a data breach:

1. In the navigation bar, click **Registers > Data Breaches**.

2. Select a data breach and in its property page, select the **Breach Assessment** page.

Here you can:

- write about the consequences of the data breach
- create remediation actions
- assign the person responsible for the management and follow-up of the data breach

☛ *For more information, see Planning Remediation actions.*

Planning Remediation actions

You need to take adequate measures to avoid data breach.

To create remediation actions:

1. In the navigation bar, click **Registers > Data Breaches**.
2. Select a data breach and in its property page, select the **Breach Assessment** page.
3. Under **Remediation actions**, click **New**.
4. Enter a comment describing how to remediate the data breach.
5. Specify the status of the remediation action:
   - Foreseen
   - Implemented
   - Ongoing

   ☛ *You can modify the status later on.*
6. Click **OK**.

Notifying a Data Breach

It may be necessary to inform supervisory authorities or data subjects when a data breach occurs. If so, please detail how the notification is handled.

To give information about data breach notification:

1. In the navigation bar, click **Registers > Data Breaches**.
2. Select a data breach and in its property page, select the **Breach Notification** page.

You can indicate whether the data breach requires:

- **data subject notification**

  ☛ *Enter a **Data subject notification date**.*
- **supervisory authority notification**

  ☛ *Specify the:*
  - ***Notified supervisory authorities***
  - ***Privacy authorities notification date***

Viewing Elapsed Time since Breach Discovery

Under data privacy laws, you have a specific number of hours to take action on detection of the breach and notify authorities or data subjects.

Hopex Privacy Management automatically computes this piece of information for you.

To view the number of hours which have passed since breach discovery:

1. In the navigation bar, click **Registers > Data Breaches**.
2. From the list of data breaches, select the breach of interest to you and view the content of the column **Hours from breach discovery**.

Duplicating Data Breaches

You may want to duplicate data breaches.

To do so:

1. In the navigation bar, click **Registers > Data Breaches**.
2. From the list of data breaches, select the breach of interest to you and click **Duplicate**.
3. In the wizard that appears, select the sections you want to duplicate and click **OK**.

MANAGING DATA SUBJECT REQUESTS

Data privacy laws give data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller.

A data subject request is a formal request by a data subject to a controller to take action on his/her personal data.

The law requires the data controller to keep a record of all data subject requests. **Hopex Privacy Management** enables you to do so and to ensure follow-up with undue delay.

Creating a Data Subject Request

You need to record the data subject requests received.

To create a data subject request:

1. In the navigation bar, click **Registers > Data Subject Requests**.
2. Click **New**.

You must specify the following information:

- **Request Status**
  - Pending Request
  - New
  - Assigned
  - Processing
  - Closed
- **Request Type**
  - Access

    📖 Right to Access entitles the data subject to have access to and information about the personal data that a controller has concerning them.
  - Deletion

    📖 A data subject may also have the right to have you delete data that you keep on him or her.
  - Objection

    ☛ The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her
  - To be forgotten

    📖 The Right to be forgotten is also known as Data erasure. it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.
  - Rectification

    ☛ The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
  - Portability

    📖 Data Portability is the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.
  - Restriction

    ☛ The data subject shall have the right to obtain from the controller restriction of processing.
- **Request Date**

  ☛ It is mandatory to specify the request date. This date will help automatically compute the number of days which have passed since the data subject request.
- **Data Subject Name**

Specifying Information on a Data Subject Request

To further describe a data subject request, you can add the following information:

- **Data Subject Request**

  ☛ A comment can be entered here.

- **Request source**
  The request source is the means through which the request is received.

  `Example: the ID of a web form`

- **Request Priority**
  - High
  - Medium
  - Low
- **Assigned person**
- **Data Subject Category**
- **Document type**
  It is important to record an official document to officially identify the data subject. This document may be:
  - an ID
  - a passport
  - a driving license
  - other
- **Document number**: corresponds to the number of the document selected above
- **Tag**

  ☛ Tags can be selected to facilitate full text search. For more information on tags see Collaboration features.

Describing the Scope of a Data Subject Request

It is necessary for you to describe the scope of the data subject request, i.e. which legal entities and departments are impacted by the data subject request. You may also want to get into the details and specify a related processing activity.

To describe the scope of a data subject request:

1. In the navigation bar, click **Registers > Data Subject Requests**.
2. In the property page of a data subject request, select the **Request Scope** tab.
3. From the drop-down lists available select the impacted:
   - legal entities
   - departments
   - and/or processing activities

   ☛ Please note that the number of data subject requests by legal entity/department is an important criteria, as this may constitute a Key Performance Indicator in business matters.

Attaching Documents to the Data Subject Request

It may be useful to provide any relevant attachment that can help further describe the data subject request (eg. a copy of the email used to send the request).

To attach a document to the data subject request:

1. In the navigation bar, click **Registers > Data Subject Requests**.
2. In the property page of a data subject request, select the **Attachments** tab.
3. Create an attachment and specify:
   - a document ID
   - a document title
   - the document description
4. In the **File Location**, select the document to attach.
5. **Upload** and click OK.

Managing Data Subject Management Deadlines

The number of days which have passed since the data subject request is automatically computed.

As the deadline of 30 days approaches, if the status of the data subject request is not set to "closed", the person in charge of the request management is notified by email.

After 30 days, you may indicate you want this period to be extended, as authorized by the law.

To extend the deadline of the data subject request:

1. In the navigation bar, click **Registers > Data Subject Requests**.
2. In the columns available on the data subject request, select the **Deadline extended** check box.

MANAGING ACTION PLANS

Within the framework of **Hopex Privacy Management** action plans can be used to:

- Implement remediation action following DPIA results
- Manage data breaches
- Manage data subject requests

Managing action plans consists in defining, executing and following up a certain number of actions.

ACCESSING ACTION PLANS

Accessing all Action Plans

To access action plans in **Hopex Privacy Management**:

- In the navigation bar, select **Action Plans**.

Here you find the list of action plans and actions sorted according to different criteria.

Action Plans

This tab displays all the action plans.

From the drop-down list you can select the **Action plans to implement** only.

Actions

- **Actions by action plans**
  - ☛ *This tab displays a tree of actions classified by action plan.*
- **Actions to implement**
  - ☛ *This tab displays the list of actions you need to implement.*
- **Actions to implement by action plan**
  - ☛ *This tab displays a tree of the actions you need to implement, classified by action plan.*

Accessing Action Plans specific to a Processing Activity

To access action plans specific to a processing activity:

1. In the navigation bar, select **ROPA**.
2. Open the property pages of a processing activity and select the **Action Plans** page.

DEFINING ACTION PLANS

To define an action plan:

1. See Accessing Action Plans.
2. Open the properties of the action plan of interest.

General Characteristics

In the **Characteristics** section, you can specify action plan fields, for example:

- **Name**: action plan name.
- **Owner**: is by default the user who created the action plan.
- **Tags**
- **Owner Entity**: enables restriction of the list of owners.
- **Approver**: user responsible for validation of the action plan when all actions are completed.
- **Means**: text description of means required/desired for action plan execution.
- **Priority**: enables indication of a level. Priority can be:
  - "Low",
  - "Medium"
  - "High"
  - "Critical"
- **Origin**: enables definition of the context of carrying out the action plan:
- **Category**: enables specification of the action undertaken.
- **Nature**: enables definition of the action plan undertaken:
  - "Preventive"
  - "Corrective"
- **Description**: supplements information on the action plan and its characteristics.
- **Steering calendar**: enables to define the frequency for progression reminders.

Financial Assertions

- **Forecast Cost**: estimate of action plan cost expressed in **Currency**.
- **Forecast Cost (Man-Days)**: estimate in man-days of action plan implementation workload.
- **Real Cost**
- **Real Cost (Man-Days)**

Success Factor and Outcomes

In the **Success Factors** section, you can enter performance indicators enabling to assess action plan completion.

- **Key Success Factor**: text information on action plan success factors.
- **Outcome**: information on action plan final success.
  - "Unknown"
  - "Failed"
  - "Succeded"
- **Comments on Outcome**: text information on action plan results.

Scope

In **Hopex Privacy Management**, the action plan needs to be positioned on a processing activity.

Milestones

Milestones are important dates. You can specify these dates later.

- **Planned Begin Date**
- **Planned End Date**

Attachments

You can attach business documents to an action plan:

☛ *For more details on the use of business documents, see the **Hopex Common Features** guide.*

MANAGING ACTIONS

Actions enables you to break down action plans into elementary items. These actions can be assigned to different stakeholders and implemented through a workflow.

To create and assign actions:

1. See Accessing Action Plans.
2. Open the properties of the action plan.
3. In the **Actions** section, click **New**.
4. Open the properties of the action and specify its **Name**.
5. Specify the following fields:
   - **Owner**: responsible for the action as specified by the action plan creator.
   - **Owner Entity**: owner organization unit enabling restriction of the list of action owners.
6. In the **Milestones** section, specify important dates for the action.
   - **Planned Begin Date** and **Real Begin Date**.
   - **Planned End Date** and **Real End Date**.
7. Click **OK**.

See Action Workflow.

ENSURING ACTION PLAN FOLLOW-UP

Action plan progress is specified at periodic dates by the action plan responsible user. For more details, see Specifying Action Plan Progress Update.

So that a reminder e-mail can be automatically sent to the action plan responsible user, you can connect a **Steering Calendar** to the action plan. For more details, see Using Steering Calendars.

Specifying Action Plan Progress Update

The action plan progress rate can be specified if the action plan is in the status "In progress", that is it has been validated.

To indicate progress for an action plan:

1. Open the properties of the action plan and expand the **Progress History** section.
2. In the **Progress Update** section, click **New**.
   The **Creation of Progress Update** page appears.
3. Specify the **Progress (Percentage)** and add a **Description**, if required.
4. Verify the **Progress Date**.
5. Specify the **Progress Evaluation**.
   - On Time
   - Late
6. Click **OK**.
   The progress update appears in the list.

Using Steering Calendars

You can connect a **Steering Calendar** to the action plan so that the action plan responsible user can indicate a progress percentage at dates defined in this calendar. A message is sent to the user on these dates.

> ☛ *For more details on managing steering calendars, see **Platform Customization (Windows) - Customizing Steering calendars**.*

To connect a steering calendar for an action plan:

1. Open the properties of an action plan.
2. In the **Characteristics** section, click the arrow at the right of the **Steering Calendar** field.
3. Select a steering calendar.

> ☛ *There is a default steering calendar for action plans but you may choose your own customized steering calendar.*

MONITORING ACTION PLAN PROGRESS

To be able to monitor the progress of a specific action plan:

1. See Accessing Action Plans.
2. Open the properties of an action plan and select the **Progress Report** page.

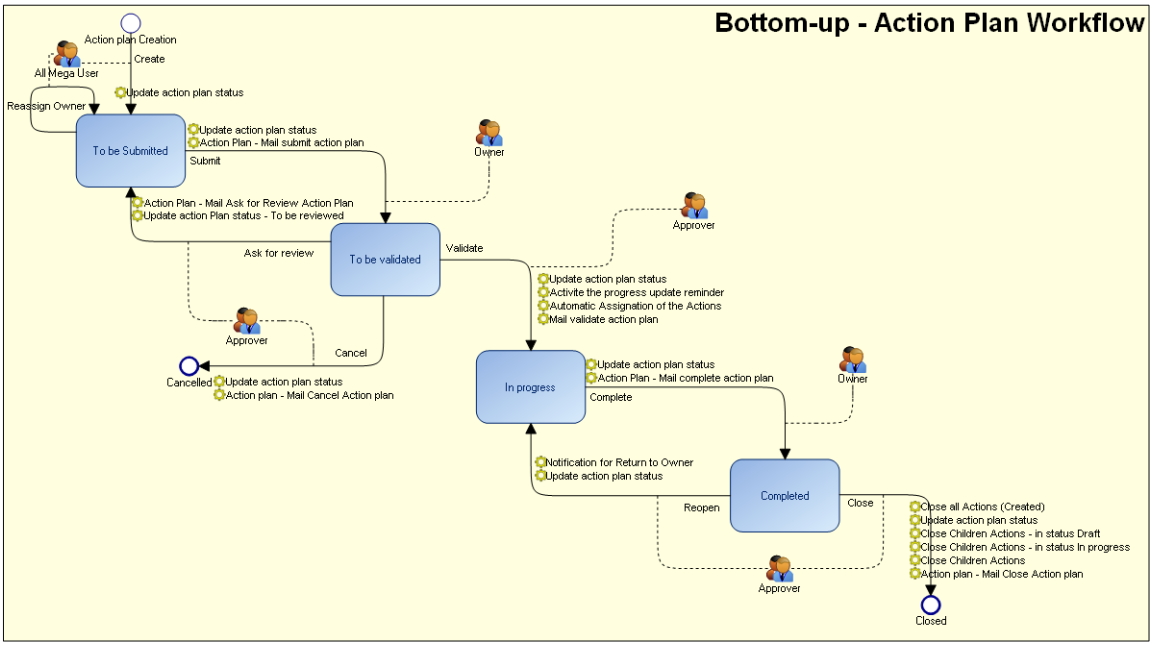
This report displays a Gantt of actions as well as the progression history of the action plan.

APPENDIX: ACTION PLAN WORKFLOWS

Two workflows are proposed to manage the different steps of an action plan:

- A **Bottom-Up** workflow, which corresponds to the case where an action plan is created by any user, for example a processing activity owner. Here the new action plan must be validated by an approver before being implemented.
- A **Top-Down** workflow, which corresponds to the case where an action plan is created by an "action plan manager", for example the DPO.

Bottom-Up Action Plan Workflow



Creating the action plan

When an activity/application owner creates an action plan, the created action plan is in "To be Sent" state.

By default, the action plan creator is the action plan **Owner**. Having specified the characteristics of a new action plan, the creator can:

- **Propose** the action plan.
  In this case, the user defined as "Approver" receives a notification mail, and the new action plan appears with status "To Begin" in his/her tasks list.

If you changed the name of the approver (which is by default the one who created the action plan), you first need to **Reassign** the approver from the pop-up menu of the action plan.

Preparing the action plan

The action plan "Approver" user can:

- **Validate** the action plan, which then takes status ""In Progress". Actions can then be created. For more details, see Managing Actions.
- **Cancel** the action plan which takes status "Canceled".

Executing the action plan

Having executed actions relating to the action plan, the "Owner" can:

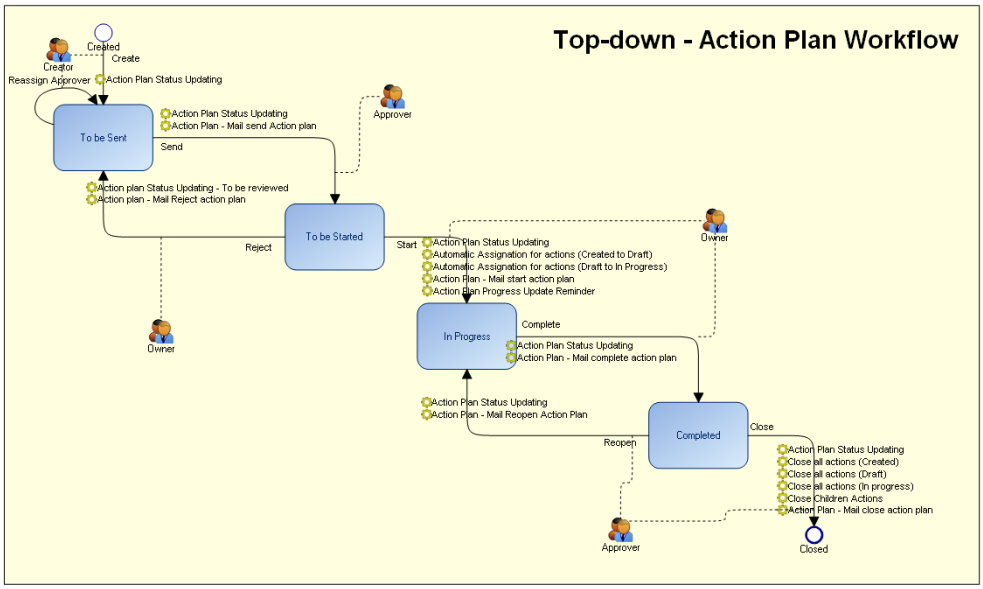
- **Terminate** the action plan which takes status "Closed". To do this, all action plan actions must be terminated. For more details, see Managing Actions.
  The "Approver" user is notified of the action plan termination request.

Closing the action plan

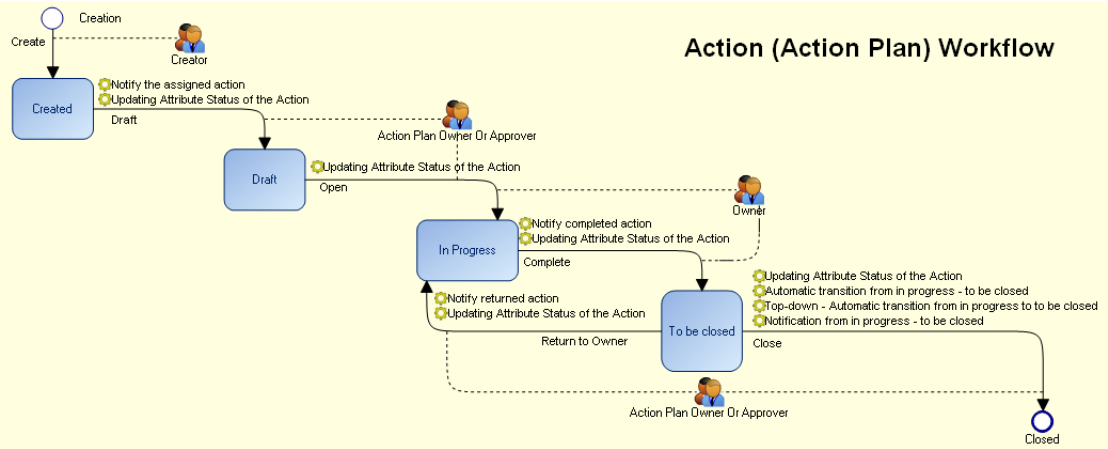
After having consulted action plan follow-up reports, the "Approver" user can:

- **Close** the action plan, which retains "Closed" status and disappears from the task lists of creator, approver and owner.
- **Reopen**, for additional actions. The action plan again takes status "In Progress".

Top-down Action Plan Workflow



Action Workflow



Notifications are sent by the creator to the responsible user:

- when the action is assigned to a user,
- when the action is closed.

DEMONSTRATING COMPLIANCE

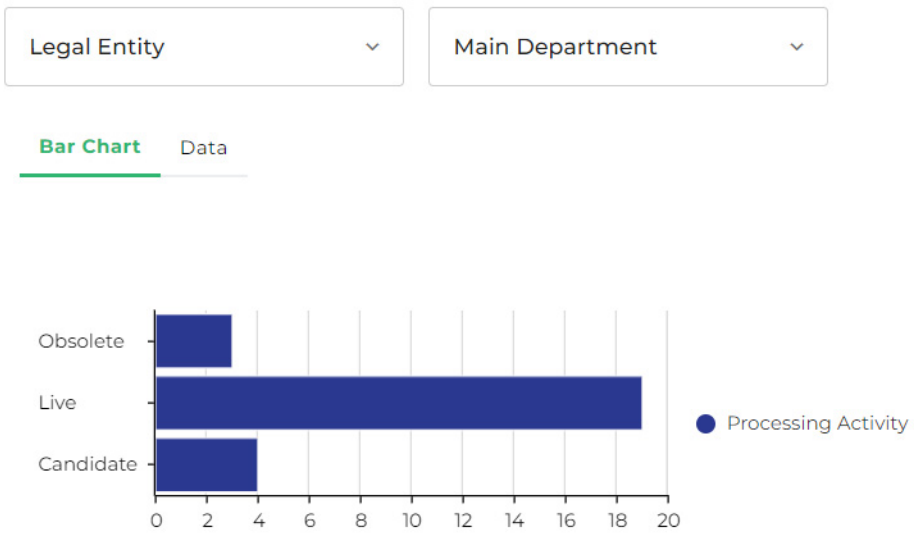
Hopex Privacy Management enables you to create reports showing the compliance and accountability level of processing activities.

To access reports:

- Select **Reports**.

Processing Activity Status

This report displays all processing activities, grouped by status, to quickly identify those requiring validation.

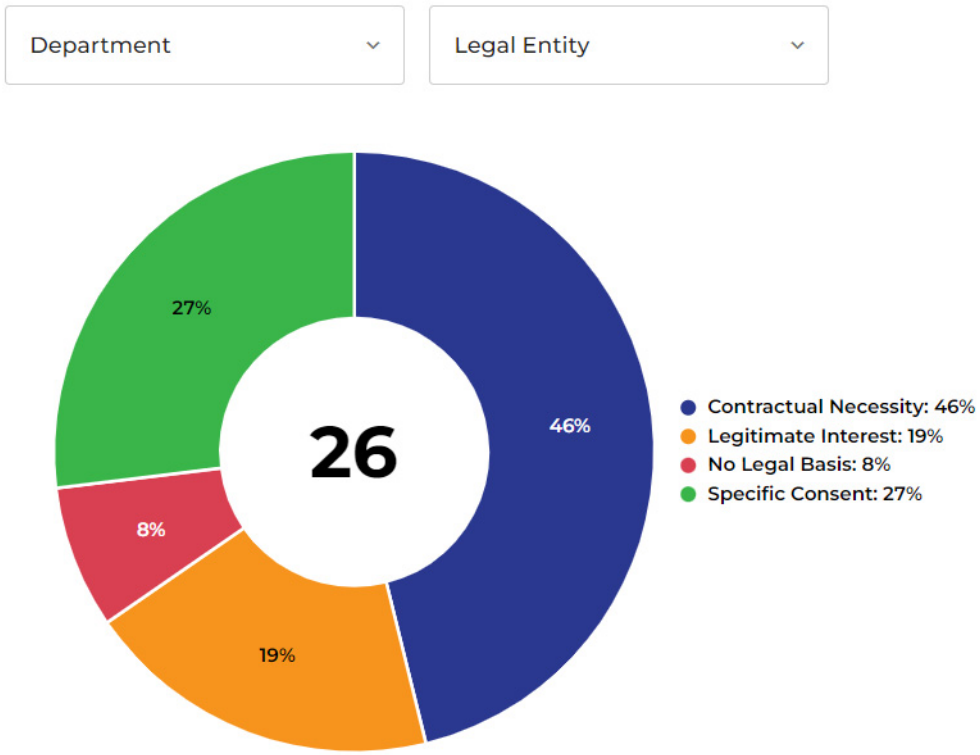


As a reminder, the following statuses are available:

- Candidate
- Live
- Obsolete

Legal Basis

This report displays the processing activities grouped by legal basis. It also helps identify those which don't have one yet.



Sensitive Activities

This report helps identify which processing activities are impacted by existing sensitive operations.

Sensitive Activity	Processing Activity	Pre-Assessment	Risk Level	Compliance Level	DPIA	Final Risk Level	Final Compliance Level
Processing of data on a large scale	Promotional activities and leads generation						
	SMS Advertising						
	Customer Relationship Management Campaigns	12/19/2018	Medium	Almost Compliant		Medium	Almost Compl
	Call Center Outbound		High	Compliant	12/19/2018	High	Compliant
	Call Center Outbound	1/7/2019	High	Compliant	12/19/2018	High	Compliant
	Call Center Outbound	5/5/2023	High	Compliant	12/19/2018	High	Compliant
Processing of sensitive data or data of a highly personal nature	Collection of donations	12/19/2018	Low	Almost Compliant		Low	Almost Compl

Data Category and Data Subject Compliance

The DPO needs to produce a report with the overall risk and compliance level of all the organization processing activities.

This report contains two tables:

- one for data categories

  ☛ *For more information, see Defining Data Categories.*

Data Category	Default Data Risk Level	Processing Activity	Pre-Assessment	Risk Level	Compliance Level	DPIA	Final Risk Level	Final Compliance Level
Connection data	Medium	Customer Relationship Management Campaigns	Yes (12/19/2018)	Medium	Almost Compliant	No		
Criminal convictions or offenses	High	Commissions for agents	Yes (6/20/2022)	Medium	Almost Compliant	No		

- the other for data subject categories.

  ☛ *For more information, see Data Subject Categories.*

Data subject category	Default Data Risk Level	Processing Activity	Pre-Assessment	Risk Level	Compliance Level	DPIA	Final Risk Level	Final Compliance Level
Agents	Medium	Customer Relationship Management Campaigns	Yes (12/19/2018)	Medium	Almost Compliant	No		
Clients	Medium	Clients claims management	Yes (12/18/2018)	Low	Compliant	No		
		Customer Relationship Management Campaigns	Yes (12/19/2018)	Medium	Almost Compliant	No		
		Call Center Outbound	Yes (5/5/2023)	High	Compliant	Yes (2/6/2024)	High	Poorly Compliant
		Subscription Purchase Conditions and Privacy	Yes (6/20/2022)	Medium	Compliant	No		
		Collection of donations	Yes (12/19/2018)	Low	Almost Compliant	No		
Employees	Medium	Employees presence detection	Yes (1/2/2019)	Very High	Poorly Compliant	Yes (1/2/2019)	Low	Compliant
		Disciplinary Measures and Conciliation	Yes (12/18/2018)	Low	Compliant	No		
		Email box management	Yes (1/2/2019)	High	Poorly Compliant	Yes (1/2/2019)	Medium	Almost Compliant

Both reports display compliance and risk level of the processing activities involving each data category and data subject category. The tables distinguish between pre-assessment and DPIA results.

☛ *You can generate a report in MS Word format by clicking the corresponding icon at the report level.*

Data Transfer Map

This report displays all data transfers of personal data, grouped by destination, highlighting personal data sent to unsafe countries.

☛ *To build a map displaying data transfers, see Cross-border Transfer Map.*

Third-Parties

This report contains a list of third parties involved in existing processing activities.

Pre-requisites

For the processing activities to be displayed in this report, you must have created processing elements of "Third-Party" type.

See Creating a processing element.

Third-party report content

It gives the following information for each third-party:

- Processing activity
- Inherent risk
- Compliance level
- Last assessment date of the processing activity

Third-Party Name	Processing Activity	Inherent Risk	Compliance Level	Last Assessment Date
Salesforce	Performance Management			
	Subscription Purchase Conditions and Privacy	Medium	Compliant	6/20/2022
Adobe	Talent Program			
Alphabet	Talent Program			
American Express	Management of relations with banks	Very High	Not Compliant	6/20/2022
Oracle	SMS Advertising			
Mastercard	Management of relations with banks	Very High	Not Compliant	6/20/2022
Visa	Management of relations with banks	Very High	Not Compliant	6/20/2022
Deloitte	Call Center Outbound	High	Poorly Compliant	2/6/2024
Pardot	Market research			
	Promotional activities and leads			

The report distinguishes between:

- active third-parties
- obsolete third-parties

Data transfer map

To generate the data transfer map:

- Select the transfers of interest to you and click 

See Cross-border Transfer Map for a description of this report.

IT Applications

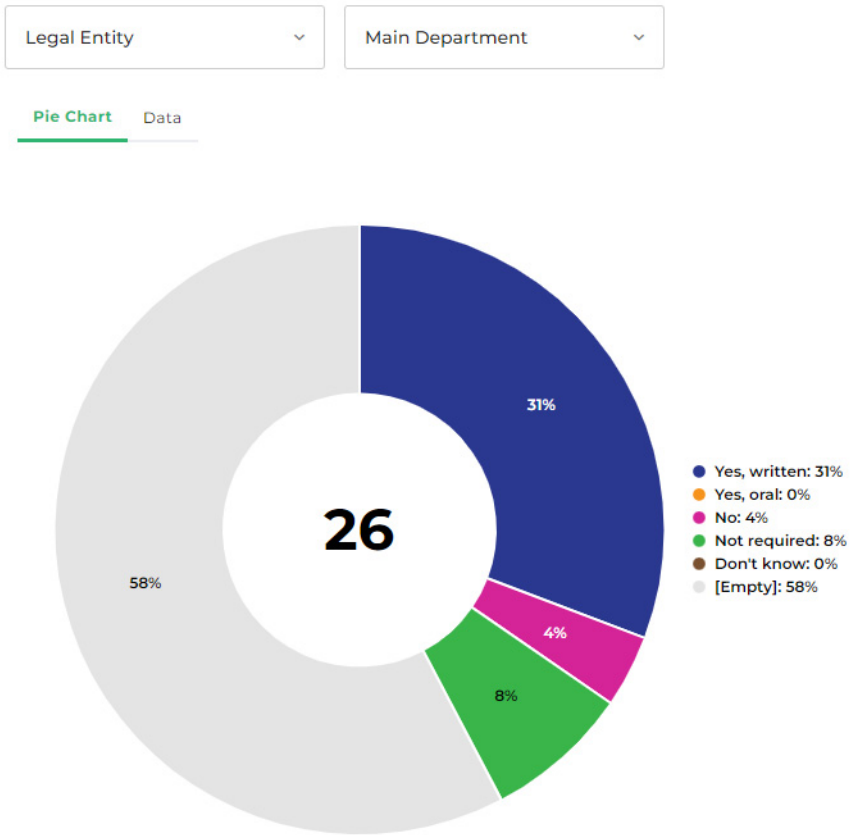
This report contains a list of all IT applications involved in the existing processing activities.

Processing Activity

Processing Activity	Processing Element	Application Name
Call Center Outbound		
Clients claims management		
Collection of donations		
Commissions for agents		
Credit Recovery	Account Payable	Account Payable
	Account Payable	Account Payable
	Account Payable	Account Payable
Customer Relationship Management Campaigns	Sending out emails and manage campaigns	
	Billing (FR)	Billing
Customer Satisfaction Questionnaires		
Disciplinary Measures and Conciliation		
Email box management	Office 365	

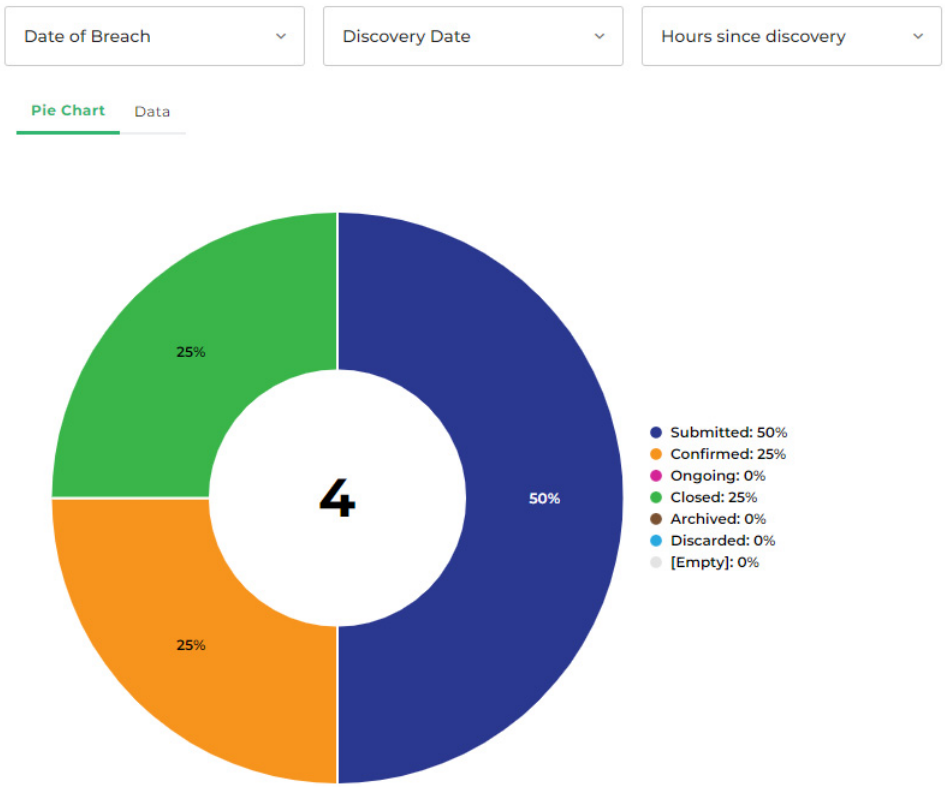
Notice

This report helps identify the processing activities without an existing notice.



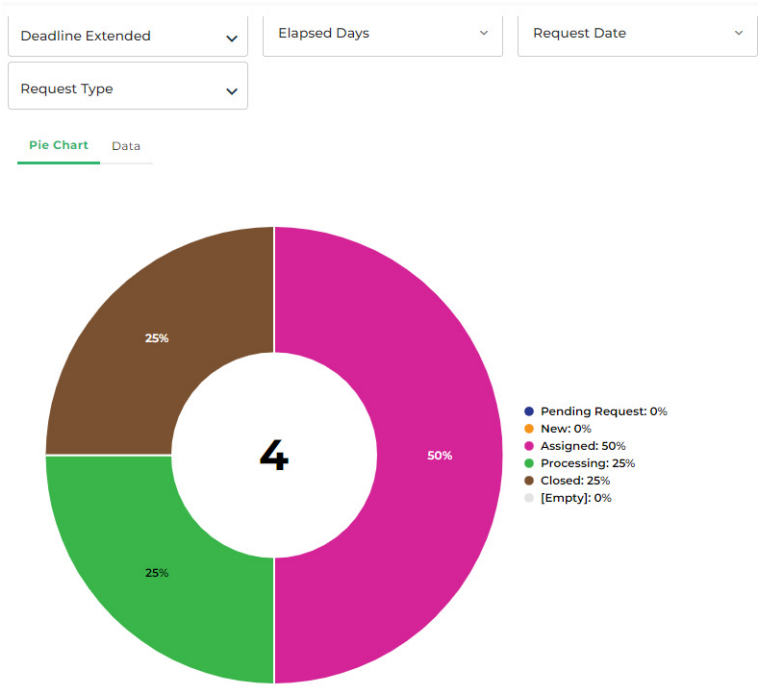
Data Breaches by Status

This report displays all data breaches, grouped by status, in order to quickly identify those requiring immediate action.



Data Subjects' Requests by Status

This report displays all data subjects' requests, grouped by status, in order to quickly identify those requiring immediate intervention.


Deadline Extended
Elapsed Days
Request Date
Request Type
Pie Chart
Data
25%
4
50%
25%
Pending Request: 0%
New: 0%
Assigned: 50%
Processing: 25%
Closed: 25%
[Empty]: 0%

FAQs

About Data Privacy

What is personal data?

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Examples of personal data:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- an Internet Protocol (IP) address

☛ *Anonymized data, or a company registration number are NOT considered personal data.*

Example of supported law

The General Data Protection Regulation (GDPR) is a European law directly applicable as of May 25th 2018 in all European member states.

Click here for official information on the GDPR.

Click here for the full text of the regulation.

☛ *This is only an example, as **Hopex Privacy Management** supports all kinds of data-protection laws.*

About Processing Activities

☛ *For general information on processing activities, see Describing Processing Activities.*

Why can't I create a processing activity?

The functional administrator must have assigned you to a department.

For more information, see Connecting Users to a department.

Why is the dashboard of my processing activity empty?

The indicators displayed at the top of the **Overview** tab of the processing activity remain gray/empty until you perform a pre-assessment or a DPIA.

For more information, see Processing Activity Dashboard.

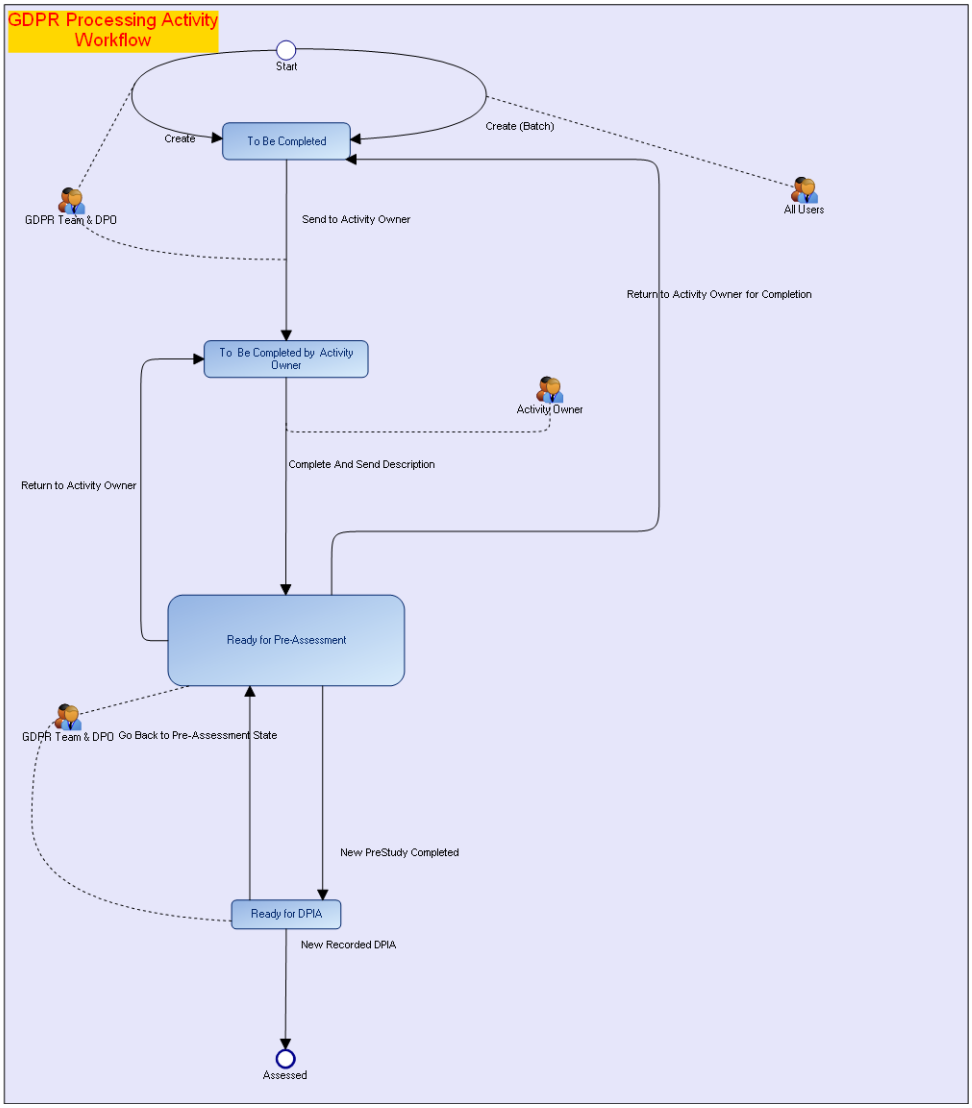
How can I produce a Word version of my record of processing?

See Creating a record of processing.

An application is used in one of my processing activity. How to describe how to handle this part of the processing activity?

Hopex Privacy Management enables you to describe processing elements of application type. For more information, see Managing Processing Activity Elements.

What are the possibilities offered by the standard processing activity workflow?



About Assessments

☛ *For more information on assessment, see Assessing Processing Activities.*

How do I know which processing activities need to be assessed?

To identify the processing activities you need to assess, we suggest you to take a look at the following:

- the ***compliance level*** of your processing activities
  - see Viewing the Initial Compliance Level of a Processing Activity

    ☛ *This information concerns the processing activity before any proper assessment is made.*
  - see Performing the Pre-Assessment

    ☛ *This information concerns the processing activities which have already been assessed.*
- the ***final risk level*** of your processing activities

  ☛ *See Performing the Pre-Assessment*
- the ***assessement status*** (DPIA)

  ☛ *See Performing the Pre-Assessment*.

Is it possible to carry out a DPIA outside the solution?

Yes, it is possible.

We suggest you to proceed as follows to reference the DPIA in **Hopex Privacy Management**:

1. Create a DPIA without adding risks or recommendations.
2. Attach your external DPIA.
3. Fill in the validation levels and specify what needs to be done next.

   ☛ *For more information on DPIA creation, see Performing Impact Assessment (DPIA).*

How can I produce a Word version of a DPIA?

You have two ways to generate a Word document out of your DPIA:

- From **Reports > Record of DPIAs**.

  ☛ *For more information, see Data Category and Data Subject Compliance.*
- From the **DPIA** page of the processing activity properties.

  ☛ *For more information, see Generating a DPIA document.*

Some of my processing activities are similar. Can I reuse an existing DPIA?

Yes, you can. You can duplicate a processing activity then make the necessary changes.

☛ *For more information, see Reusing a DPIA.*

How is the Final Compliance Level computed?

☛ *This field is available in the **Preassessment** or **DPIA** page of a processing activity. See Performing the Pre-Assessment.*

See also Specifying Compliance Levels.

Final Compliance Level: sum of conformance levels / 5. The result is rounded to the closest (and highest) integer.

☛ *Compliance levels can be specified on the following:*

- *Legal Basis*
- *Data Minimization*
- *Data Subjects' rights & Notice Management*
- *Data Transfers*
- *Security Measures*

In the example below, final compliance level = (10+10+10+5+5)/5 = 8

Compliance Levels				
Legal Basis	Data Minimisation	Data Subjects' Rights & Notice Management	Data Transfers	Security Measures
10	10	10	5	5

Risk Label/Value	Compliance Label/Value
Very Low - 0	Not Compliant - 10
Low - 1	Poorly Compliant - 5
Medium - 3	Almost Compliant - 3
High - 5	Compliant - 2
Very High - 10	Strongly Compliant - 1

Pre-Assessment		
Final Compliance Level	Final Risk Level	Subsequent Action
8	7	

DPIA		
Final Compliance Level	Final Risk Level	Subsequent Action
8	7	

Let's compare the result obtained with the possible compliance level values:

8 is closer to 10 (Not compliant) than 5 (Poorly compliant)

-> Final Compliance Leval = Not compliant

Compliance Label/Value
Not Compliant - 10
Poorly Compliant - 5
Almost Compliant - 3
Compliant - 2
Strongly Compliant - 1

How is the Final Risk Level computed?

☛ *This field is available in the **Preassessment** or **DPIA** page of a processing activity. See Performing the Pre-Assessment.*

See also: How is the Final Compliance Level computed?

Final Risk Level: Final Compliance Level -1

The result is rounded to the closest (and lowest) integer.

If Final Risk Level = 7, Final Risk Level = "High" as 7 is closer to 5 (High) than 10 (Very High)

Risk Label/Value
Very Low - 0
Low - 1
Medium - 3
High - 5
Very High - 10

How is the "Subsequent Actions" field computed?

☛ *This field is available in the **Preassessment** or **DPIA** page of a processing activity. See Performing the Pre-Assessment.*

See also: How is the Final Risk Level computed?

Final Risk Level (Preassessment)	"Subsequent Actions" field value
5	Run DPIA
10	Run DPIA
Other	Other

Final Risk Level (DPIA)	"Subsequent Actions" field value
5	Notify Supervisory Authority
10	Notify Supervisory Authority
Other	Other

About Transfers

How can I create transfers?

Transfers need to be created in the **Details** tab of a processing activity.

Is there a way to view transfers graphically?

Yes, **Hopex Privacy Management** enables you to display a cross-border transfer map for a specific processing activity.

For more information, see:

- Cross-border Transfer Map.
- Specifying data transfers on a processing activity.

I created transfers but I cannot display the cross-border transfer map. What's wrong?

See Pre-requisites to using cross-border transfer map.

☛ *Also, make sure you refreshed the report after creating transfers on processing activities.*

About Hopex Privacy Management Import and Hopex Integration

How can I reuse information from other Hopex solutions?

Hopex Privacy Management enables you to:

- import applications and processes
- reuse them to create processing activities

  ☛ *For more information, see Creating Processing Activities through Duplication.*
- view application/process properties and associated diagrams directly from **Hopex Privacy Management**.

I cannot manage to drag-and-drop a sub-process under a department. What's wrong?

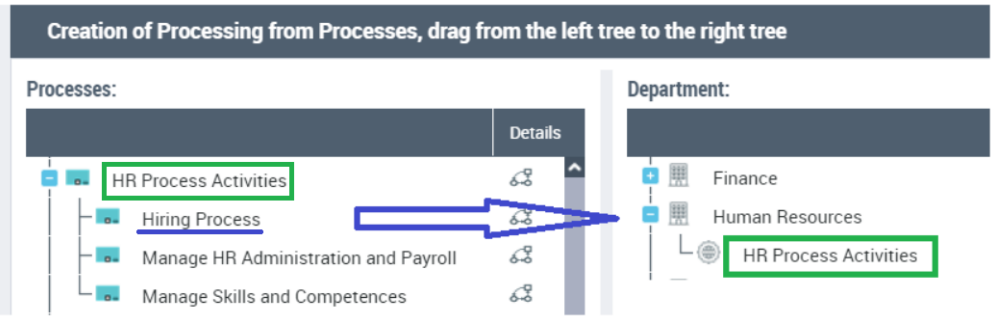
It is possible to drag-and-drop sub-processes to create a processing activity but there is a specific rule for it:

When you drag a sub-process under a department, it actually drops the parent process (not the sub-process).

Let's take an example to better illustrate the case. Let's assume that:

- there are 3 sub-processes under a process in the left tree.

- you drag-and-drop one of these sub-processes under a department in the right tree.



In the above example, "Hiring Process" gives birth to "HR Process Activities".

Now you want to drag-and drop another sub-process under another department. In our example, you might want to drop "Manage Skills and Competences" under "Finance".

-> You get an error message stating: "the sub-process cannot generate a processing as it is already connected to a processing".

Miscellaneous

Is it possible to view the diagram of an imported process?

Yes, you can if the process has been imported together with the diagram.

To do so:

1. Select **ROPA**.
2. Open the processing activity property page.
3. Click the **Details** tab then **Details View**.
   Next to the processing activity/sub-processing concerned, a button enabling you to display the diagram is made available.

   ☛ *You can also access the static web site of the process if it has been imported in **Hopex Privacy Management**.*

My DPO organizational chart is empty. What should I do?

You can draw the DPO organizational chart by specifying the hierarchy of DPOs in the entity property pages.

See Defining Legal Entity Properties. You must fill in the **DPO** and **Reporting to DPO** fields so that the organizational chart could be automatically generated.

I cannot create legal entities. What should I do?

Only the Privacy functional administrator can create legal entities or departments.

Make sure you are connected with the appropriate profile.

PRIVACY GLOSSARY

Action	An action is included in an action plan and represents some transformation or processing in an organization or a system.
Action Plan	An action plan comprises a series of actions, its objective being to reduce risks and events that have a negative impact on company activities or to improve a process or an organization efficiency.
Processing Activity Owner	The processing activity owner provides a detailed description of the processing activity (excluding assessment).
Binding Corporate Rules (BCRs)	BCRs are a set of binding rules put in place to allow multinational companies and organizations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organization).
Computing Device	Computing devices are hardware pieces that can host and run software. Together with their hosted applications, they provide Information and IS services.
Policy Document	Policy documents enable you to attach documents or specify a URL concerning privacy-relevant information the organization might use to give evidence of the company accountability.
Consent	Consent is a freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.
Data Category	Data category is used to group different personal data.
Data Controller	A data controller is the entity that determines the purposes, conditions and means of the processing of personal data.
Data Erasure	See Right to be forgotten.

Data Portability	Data Portability is the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.
Data Processor	A Data Processor is the entity that processes data on behalf of the Data Controller.
Data Protection Authority	The Data Protection Authority is a national authority tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.
Data Protection Officer	The Data Protection Officer (DPO) is an expert on data Privacy who ensures that an entity is adhering to the policies and procedures set forth in the data privacy law.
Data Subject	A Data Subject is a natural person whose personal data is processed by a controller or processor.
Data Transfer	Under a data privacy law, a data transfer is a transfer or copy of personal data.
DPIA	A data protection impact assessment (DPIA) is a privacy-related impact assessment whose objective is to identify and analyze how data privacy might be affected by certain actions or activities. Under a data privacy law, data protection impact assessments are mandatory in certain cases such as profiling.
Data Subject Category	A Data Subject category is a type of stakeholder which interacts with your organization in the context of the enterprise architecture environment, such as private sector customer, a supplier.
Data Subject Request	A data subject request is a formal request by a data subject to a controller to take action on his/her personal data.
Establishment	An establishment corresponds to the location (site) of a legal entity.
IT Support Correspondent	An IT support correspondent is in charge of providing IT support.
Joint Controller	Joint controllers can work jointly to determine the purposes and means of a processing activity.
Legal Entity	A Legal Entity is a company or an organization which has legal rights and obligations.
Minimization	Minimization is a principle stating that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

National Representative	A National Representative is a representative of the legal entity in one of the Member States. Typically, a non-European legal entity should appoint national representatives in all European Member States where there are data subjects whose personal data is processed by the legal entity.
Organizational Chart	An organizational chart contains the hierarchical structure of the organization DPOs. It shows the relationship between the appointed DPOs and helps identifying the responsibilities within the organization. It is automatically populated based on the information provided on the legal entities.
Personal Data	Personal Data consists of any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person.
Personal Data Breach	Personal Data Breach is a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data.
Physical Archive	A physical archive corresponds to the premises in which historical records are located.
Privacy by Design	Privacy by Design is a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.
Processing Activity	A processing activity consists of any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.
Profiling	Profiling consists of any automated processing of personal data intended to evaluate, analyze, or predict data subject behavior.
Purpose	The purpose of a processing activity is the main objective of this processing activity. Examples: satisfaction survey, customer management, site monitoring.
Record of Processing Activities	A record of processing activities must include significant information about data processing, including data categories, the group of impacted people, the purpose of the processing and the data receivers. It must be provided to authorities upon request.
Regulation Framework	A regulation framework is a set of directives, compulsory or not, defined by a governement in a law, by standard bodies as 'best practices' or as an internal policy in an organization.
Representative	A representative is a person in the European Union explicitly designated by the controller to be addressed by the supervisory authorities.

Requirement	A requirement is a need or expectation explicitly expressed, imposed as a constraint to be respected within the context of a regulation framework.
Retention Period	A retention enables to record the time lapse in which the data personal will be stored by the organization.
Right to Access	Right to Access entitles the data subject to have access to and information about the personal data that a controller has concerning them.
Right to be Forgotten	The Right to be forgotten is also known as Data erasure. it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.
Risk	A risk represents any risk related to data privacy that should be identified and assessed during a DPIA process.
Safeguard	Safeguards are measures taken to ensure the legitimacy of data flows. They apply to transfers only.
Security Measure	Security measures are appropriate technical and organizational measures to be taken to ensure that the requirements of the regulation are met.
Sensitive Activity	A sensitive activity is an activity whose impact on the overall processing risk is important.
Supervisory Authority	A Supervisory Authority is a public authority which is established by a member state. It may be contacted by the legal entity for example to notify a data breach or to gather feedback on a processing activity DPIA.
Third Party	A Third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

APPENDIX: GDPR IN DETAILS

The General Data Protection Regulation (GDPR) introduces significant operational innovations in the management of personal data by private companies subject to the jurisdiction of Member States of the European Union. In this section, we analyze the most important novelties, highlighting the main business impacts.

- ✓ Territorial Scope
- ✓ Personal Data Processing
- ✓ GDPR Legal Roles
- ✓ Notice and Consent
- ✓ Rights of Data Subjects
- ✓ GDPR Documentation System
- ✓ Prior Consultation to Supervisory Authority
- ✓ Data Protection Assessment
- ✓ Technical and Organizational Measures
- ✓ Data Breach
- ✓ Data Transfer Abroad
- ✓ Sanctions and Damages
- ✓ GDPR-related Definitions

TERRITORIAL SCOPE

The law of each Member State applies according to the "territorial criterion": in the sense that the law of the State in whose territory the Controller has the establishment carrying out those activities in which personal data is processed (principle of establishment).

The principle of territoriality of the applicable law, substantially transposed in the Directive (Article 4.1, Directive 95/46/EC), has highlighted serious shortcomings in the system of protection of personal data in those circumstances characterized by a global approach: in particular, with regard to Internet and cloud computing.

Directive 95/46/EC could cause a serious lack of confidence in these contexts and for these limits.

Establishment Principle in the Directive

Directive 95/46/EC establishes in Article 4 what is the applicable national law by using the so-called "establishment principle"1:

- an established company (ie, carrying out activities with a permanent establishment) in one country of the European Union observes the rules on the protection of personal data of the State in which it is established (even if it processes data of individuals of nationalities different from its own);
- a company established in the territory of several EU countries must take the necessary measures to ensure compliance with the obligations imposed by applicable national law on each of these establishments.

Establishment in Different States

If a Controller has establishments in more than one Member State, it must ensure that each of them meets the requirements of applicable national law, in accordance with the "territoriality principle". This means that the principle of attraction of the entire data protection chain to the law of the State where the data controller is based, ceases to have effect when a permanent establishment is located in another EU Member State. In fact, on the basis of this principle of territoriality, if an Italian company or "foreign company" has establishments with head offices on the territory of several EU Member States, each of them - for the processing operations related to it (that is to say, within the scope of the activities carried out) - must be subject to the national law of the referenced State. With regard to electronic commerce, Directive 2000/31/EC recital (19) specifies that «in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.».

Company Chain

The territorial criterion is confirmed by Recital (18) of Directive 95/46/EC which applies the national law of the Controller established in a Member State also to the processing activities carried out by entities acting under the direct authority of the Controller (eg Processor), wherever these operations are actually realized. In view of this, if the "foreign company" assumes the role of data controller and is subject to the national law of a Member State of the Community, any support activities carried out by a legal entity established in another Member State will be subject to the law of that Community State, presumably according to the instructions given by the same Controller - foreign company.

Reference

1. Recital (19) of Directive 95/46 states: «establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities»

Establishment Principle in the Regulation

The principle of territoriality is reaffirmed in Regulation 2016/679 1. The rules of the Regulation are applicable when the processing of personal data is carried out "within the scope of activities" of an establishment of the Controller or of the Processor, situated in the territory of the European Union. In this respect, the fact that processing operations are physically carried out within the EU territory or not will not be relevant.

Establishment Notion

The concept of "establishment" involves the actual exercise of activities through a stable organization. Article 4, paragraph 16 provides a precise definition of 'principal establishment' in relation both to the Controller and to the Processor.

Effectiveness

In order to have an establishment, the activity in question - in our case the processing operation - must be carried out in the territory of the State. The coincidence of the place of establishment with that of the exercise of the activity is also clearly reflected in Directive 2000/31/EC, which reads as follows: « the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity;». [see dir. 2000/31, Recital (19)]. The reference to the establishment is factual in nature, in the sense that it «implies the effective and real exercise of activity through stable arrangements» while «The legal form of such arrangements, whether through a

branch or a subsidiary with a legal personality, is not the determining factor in that respect.»2. This concept was reiterated by Art29WP, which recalled how it should be located at the place where the Controller actually and effectively carries out his activity [see wp56].

Stability

Art29WP believes that the requirement of the establishment shall be considered as satisfied if the company has been established for a specified period of time. In the field of data protection, it does not appear that the notion of establishment necessarily presupposes that the requirement of stability is linked to an indefinite period of permanence. The ease and speed of computer and telematic operations can, in fact, enable the carrying out of significant activities in geographically remote areas and for limited periods of time, without the need for special infrastructures or investments at the site of actual processing. In any case, the rights of data subjects would be exposed to potential risks even in such circumstances. Therefore, in the field of data protection, the apparent attenuation of the notion of permanence within the definition of stability may find these justifications.

References

1. Article 3.1 Regulation 2016/679 which rephrases article 4.1 (a) Dir. 95/46/EC.

2. Recital (22) Regulation 2016/679

Foreign Company Subject to Regulation

Regulation 2016/679 contains a great deal of novelty regarding the scope of the rules contained therein; companies that direct their services to, or offer their products to, subjects who are on the EU territory, will be subject to EU discipline, regardless of the principle of territoriality [art. 3 (2)]. The same goes for monitoring the behavior of individuals in the EU.

This solution responds to the questions raised in the Internet and cloud computing contexts, as well as in all those situations where we use outsourcer chains around the world.

So, summarizing, Regulation 2016/679, for anti-elusive purposes, states that companies that

- direct the offer of goods or services, even free of charge, to individuals located in EU territory, using their personal data
- deal with personal data to monitor the behavior of individuals in the EU

are subject to the Union's data protection discipline, irrespective of whether they have an establishment on the territory of the EU [art. 3. (2) and art. 27 Reg.].

Offering of Goods or Services to EU residents

For the rules of Regulation 2016/679 to be applicable, it is sufficient for the promotion of goods and services be directed to consumers in the Union, such as through online trade, or implying the enforcement of contractual obligations that

imply the use of personal data of one of the parties in the EU. As stated in art. 3.2, lett. (a), the application of the rules of the Regulation does not require that the supply of goods or services or the performance of the contract have to be paid (recital 23).

Monitoring Behavior of EU residents

In order to determine whether the activity carried out by the Controller consists of "behavioral monitoring" - for the purposes of applying Regulation 2016/679 also for a Controller without his own establishment in the EU territory, as set out in Recital (24) - it must be verified that the processing activity is carried out within the Union and that the data subjects are traced on the Internet with techniques that apply a profile to each individual (profiling), in particular in order to take a decision on the data subject or for behavioral or predictive analysis of his or her preferences, behaviors, or attitudes.

Controller Representative or Foreign Processor

The appointment of a representative on EU territory [Recital (80) and art. 27] is prescribed for the company

- Controller or Processor
- which does not have an establishment in the EU territory
- which deals with the personal data of data subjects who are in the Union
- whose processing activities are related to the provision of goods or the provision of services to data subjects in the Union or the monitoring of their behavior within the Union

Obligation is excluded if

- the processing is occasional,
- does not include "sensitive" or "judicial" large-scale processing and is unlikely to present a risk to the rights and freedoms of data subjects, taking into account the nature, context, scope, and purpose of the processing
- the data controller is a public authority or public body.

The representative may be both an individual and a company, it is designated by a written mandate, and acts on behalf of the Controller or the Processor with respect to the obligations that derive from the regulation.

The designation of the representative does not affect the general liability of the Controller or Processor under the Regulation.

Applicability Member State Law due to International Law

Another case where the rules of the Regulation apply despite the fact that the data controller does not have an establishment located in the EU territory, is in a situation where, according to international law, the law of a State member of the EU shall be applied1.

Recital (25) proposes examples of diplomatic missions or consular posts in a Member State: "Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post."

Reference

1. See art. 3.3 Reg. 2016/679 which rephrases art.4.1 (b) Dir. 95/46/EC.

PERSONAL DATA PROCESSING

Legal Entity Data

The watershed that delimits the application scope of the Regulation is the information that identifies the legal person; this information is out of the scope of the Regulation 2016/679.

In this regard, the definition of "enterprise" contained in Regulation 2016/679 deserves attention; "enterprise" means "a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity" (Article 4 (18)].

Consequently, the line of demarcation of the objective scope of Regulation 2016/679 is not the "professional" or business nature of the information, as is the case with the consumption discipline based on the professional-consumer dichotomy; since a data referring to a company of people, to an individual entrepreneur or to a professional is still a "personal data". Therefore, the aforementioned delimitation between what is in the objective scope of the Regulation and what is left out of it, insists on the reconsiderability of the same information to the legal person (outside the scope of protection) as opposed to other information susceptible of identifying an individual (object of protection).

Common Data

The "common data" category is not coded in the Regulation but has been coined by the practice of gathering in one single container the information other than those fallin in the "special data categories", also known as "sensitive" or "judicial", identified by law and target of a particular discipline.

The "common data" / "sensitive data" dichotomy may still have some meaning after the advent of Regulation 2016/679 but sees its relevance reduced as a result of the regulatory introduction of the risk-based approach that imposes on the Controller to assess the factual situation and the related risk in relation to the rights and freedoms of the data subjects.

It follows that even so-called "common" data, in a particular context and for specific purposes, could in theory expose the related processing to specific risks for the data subjects, requiring the adoption of appropriate caution and measures similar to those found when using "sensitive data".

Special Categories of Data

Regulation 2016/679 takes into account special categories of personal data in terms of their impact on the personal sphere of the individual. In addition to sensitive data,

including health data, specific provisions are addressed to biometric data and genetic data.

Health data, biometric data and genetic data are the subject of individual definitions (Article 4, points 13), 14) and 15)].

Sensitive Data

As in Directive 95/46/EC (Article 8), sensitive data are not officially defined but are identified in the provision governing their use (Article 9). This typology is made up of the following categories of data relating to:

- Ethnic race and ethnic origin
- Political opinions
- Religious convictions and other types of convictions
- Adherence to trade unions
- Genetic data
- Health conditions
- Sex life
- Criminal offenses, restrictive measures or related penal measures.

Legitimate Conditions for Sensitive Data

Generally speaking, processing of sensitive and judicial data is prohibited. This prohibition, however, is subject to specific exceptions (Article 9) which follow the hypotheses already provided for in Directive 95/46/EC, with certain variants (Article 8).

Biometric Data

Biometric data are defined as those «relating to the physical, physiological or behavioural characteristics of» a data subject «resulting from specific technical processing» and «which allow or confirm the unique identification of that natural person», such as dattiloscopic data [art. 4 (14)]. A simple photo does not contain biometric data as it is not obtained by means of a «specific technical processing» [Recital (51)].

Genetic Data

Genetic data are defined as those «relating to the inherited or acquired genetic characteristics of» an individual «which give unique information about the physiology or the health (...) and which result, in particular, from an analysis of a biological sample» [art. 4, (13)].

Health Data

Health data finds a specific definition within art. 4, (15). They are considered as such, information about an individual's health status. The definition specifies that they concern «personal data related to the physical or mental health of a natural person, including the provision of health care services».

Sanction for Sensitive Data Breaches

Infringement related to the processing of sensitive data (Article 9) is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

Common Data

The "common data" category is not coded in the Regulation but has been coined by the practice of gathering in one single container the information other than those fallin in the "special data categories", also known as "sensitive" or "judicial", identified by law and target of a particular discipline.

The "common data" / "sensitive data" dichotomy may still have some meaning after the advent of Regulation 2016/679 but sees its relevance reduced as a result of the regulatory introduction of the risk-based approach that imposes on the Controller to assess the factual situation and the related risk in relation to the rights and freedoms of the data subjects.

It follows that even so-called "common" data, in a particular context and for specific purposes, could in theory expose the related processing to specific risks for the data subjects, requiring the adoption of appropriate caution and measures similar to those found when using "sensitive data".

Sensitive Categories of Data

Regulation 2016/679 takes into account special categories of personal data in terms of their impact on the personal sphere of the individual. In addition to sensitive data, including health data, specific provisions are addressed to biometric data and genetic data.

Health data, biometric data and genetic data are the subject of individual definitions (Article 4, points 13), 14) and 15)].

Sensitive Data

As in Directive 95/46/EC (Article 8), sensitive data are not officially defined but are identified in the provision governing their use (Article 9). This typology is made up of the following categories of data relating to:

- Ethnic race and ethnic origin
- Political opinions
- Religious convictions and other types of convictions
- Adherence to trade unions
- Genetic data
- Health conditions
- Sex life
- Criminal offenses, restrictive measures or related penal measures.

Legitimate Conditions for Sensitive Data

Generally speaking, processing of sensitive and judicial data is prohibited. This prohibition, however, is subject to specific exceptions (Article 9) which follow the hypotheses already provided for in Directive 95/46/EC, with certain variants (Article 8).

Biometric Data

Biometric data are defined as those «relating to the physical, physiological or behavioural characteristics of» a data subject «resulting from specific technical processing» and «which allow or confirm the unique identification of that natural person», such as dattiloscopic data [art. 4 (14)]. A simple photo does not contain biometric data as it is not obtained by means of a «specific technical processing» [Recital (51)].

Genetic Data

Genetic data are defined as those «relating to the inherited or acquired genetic characteristics of» an individual «which give unique information about the physiology or the health (...) and which result, in particular, from an analysis of a biological sample» [art. 4, (13)].

Health Data

Health data finds a specific definition within art. 4, (15). They are considered as such, information about an individual's health status. The definition specifies that they concern «personal data related to the physical or mental health of a natural person, including the provision of health care services».

Sanction for Sensitive Data Breaches

Infringement related to the processing of sensitive data (Article 9) is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

GDPR Legal Roles

Regulation 2016/679 clearly determines the roles and responsibilities of certain figures who are in charge of the company's data protection system.

The apex of the system continues to be that of the data controller and the Regulation specifies the boundaries of liability both in the case of a joint relationship with other controllers regarding the same processing (joint-controllers) and in relation to potential processors.

Even the figure of the processor takes on a better defined connotation, with clear and direct assumption of responsibility.

Persons who use personal data under the direct authority of the Controller or Processor must receive specific instructions from the Controller. On this regard, the Regulation 2016/679, as already set out in Directive 95/46, considers the aforementioned a specific security measure (Article 32.5).

Lastly, the role of the DPO – whose designation in certain circumstances is mandatory – has a function of monitoring the proper functioning of the system (Article 37).

The Undertaking

The undertaking is mentioned in the discipline introduced by the Regulation under several profiles:

- as potential data subject to which the information relates
- as the data controller
- as potential data processor
- as micro, small or medium-sized enterprise, which are entitled to facilitations or derogations.

Regarding the subjective scope, Regulation 2016/679 clarifies that it does not apply to «the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.» [Recital (14)].

The Enterprise as an Interested Subject

For "enterprise", according to the Regulation, "a natural or legal person engaged in an economic activity, irrespective of its legal form" [art. 4, 18)]; therefore both natural persons, such as professionals, associations and consortia who are regularly engaged in an economic activity. It follows that the enterprise which does not have legal personality still falls under the subjective scope of the safeguards recognized by Regulation 2016/679. Therefore, the criterion of discrimination for the applicability of the provisions of the Regulation from a subjective point of view, is not so much the pursuit of an economic activity (as in the perspective of consumer

law), but the fact that the enterprise the potentially identifiable information refer to has legal personality or not.

SMEs as data controllers

Regulation 2016/679 takes on board the impact that the reform framework may have on SMEs: these are identified in accordance «with Article 2 of the Annex of the Commission Recommendation 2003/361/EC» [Recital (13)].

Derogations and Facilities for SMEs

For organizations with less than 250 employees, only one exception is foreseen for the retention of the record of processing, except in certain cases (Article 30.5). The Regulation draft submitted by the Commission considered other facilitations for SMEs, which were no longer reproduced in the final version of the Regulation, such as:

- the exemption from the obligation to designate a national representative for foreign SMEs [Art. 25.2 (b) of the proposal];
- the exemption from the obligation to appoint a data protection officer [Art. 35.1 (b) of the proposal];
- the written reprimand, alternative to the administrative sanction, when the data protection activity was ancillary to the main mission of the SME and the violation was the first and it was not intentional [Art. 79.3 (b) of the proposal].

In any case, according to Regulation 2016/679, «the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.» [Recital (13)].

NOTICE AND CONSENT

Transparency

As in Directive 95/46/EC, also in Regulation 2016/679, the transparency of the processing activities of the Controller constitutes a major element of the general protection system (Articles 12 to 14).

The data subjects must be made aware in particular of the processing operations and their purposes, the obligation or not to provide the data and the consequences in case of refusal, the duration of the data retention, the presence of access rights, rectification or cancellation and the possibility of lodge a complaint to the supervisory authority or a direct action to the judicial authority.

In order to carry out its functions, transparency must be met prior to processing, that is to say, when collecting data, except for specific exceptions.

Notice:Contents

Similarly to the provisions of Directive 95/46/EC (Articles 10 and 11), Regulation 2016/679 requires the notice to provide an exhaustive content.

Therefore, according to the Regulation, the notice must contain:

- contact data of the Controller and, if present, of his representative as well as the DPO
- indication of the purpose pursued and of its legal basis
- specification of the legitimate interest of the Controller when the processing is based on that assumption
- recipients or categories of recipients of the data
- the intention of the Controller to carry out cross-border data flows beyond EU borders, the reference to a decision on the adequacy of the data protection scheme of the foreign country to which the personal data may or may not be transferred (or an indication of its absence), and any measures to safeguard such data flow (such as SCC and BCR) as well as the means to obtain a copy of the data or the place where they are available.

In compliance with the principles of transparency and fairness it is also necessary to provide these additional information to the data subjects:

- specification of the data retention time or of the criteria used to determine it;
- specifying the right of access and other data subjects' rights;
- clarification of the revocability of the consent at any time without any retroactive effect;
- the right of the data subject to lodge a complaint with the supervisory authority;
- the existence of the obligation to provide the data and the consequences in case of refusal, if the supply of the data results from a legal or contractual obligation;
- the existence of an automated decision, including profiling, as well as information on the underlying logic and the consequences for the data subjects (Article 13).

Notice:New Rules

The amendments introduced by Regulation 2016/679 with respect to the mandatory information that the notice must contain under Directive 95/46/EC are as follows:

- the contact details of the DPO, if present
- the legitimate interest of the Controller, when that element constitutes the basis for the validity of the processing
- the level of protection provided by the foreign country to which the Controller intends to transfer the personal data
- the data retention period or the criteria for determining it
- the revocability of consent at any time
- the right to lodge a complaint with the supervisory authority.

If the data are collected directly from the data subject, it will be necessary to specify whether the data supply is compulsory or optional and what are the consequences of the refusal [art. 14.2.e)].

Finally, when the data collection does not happen in presence of the data subject, the latter must also be informed about the source of the acquisition of the information (Article 14.3).

Sanctions for omitted notice

Violation of the obligation to provide the notice or the usage of inappropriate notices is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

Notice:Exceptions

Exceptions to the obligation to provide the notice under Regulation 2016/679 (Articles 13.4 and 14.5) are essentially those already contained in Directive 95/46/EC.

Personal data collected from data subject

In the case of personal data directly collected from the data subject, paragraph 4 of art. 13 recognizes the possibility of omitting the notice if the data subject has already been informed.

Personal data not obtained from the data subject

If, on the other hand, the information was collected by other means, paragraph 5 of art. 14, reads:

> "Paragraphs 1 to 4 shall not apply where and insofar as:
>
> (a) the data subject already has the information;
>
> (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
>
> (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
>
> (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy."

Notice:When to be Issued

The notice must be provided to the data subject in different moments, based on whether the personal data are collected directly from the data subject or from third parties.

In case of direct collection, the notice must be given:

- when collecting data, (Article 13.1).

In case of collection from third parties, the notice to the data subject must be given:

- within a reasonable period of time after collection, but not more than one month, taking into account the circumstances of the case [art. 14.3, lett. to)]
- when it is expected that the data will be communicated to the data subject, not later than the first communication [art. 14.3, lett. b)]
- in case of foreseen communication to third parties, not later than the first communication [art. 14.3, lett. c)].

Consent

One of the main sources of legitimacy in the processing of personal data is the explicit consent of the data subject [art. 6.1, lett. to)].

It must be unambiguous and informed [art. 4.11)]. The criterion of unambiguity reproduces the former wording of Directive 95/46/EC [Art. 7, lett. a)]. This formulation was the subject of the opinion wp187, expressed by Art29WP.

Sanctions for consent violations

Violation of the obligations regarding consent and its requirements as a prerequisite of lawfulness (Articles 6, 7 and 9) is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

Consent Lawfulness Conditions

Concerning data subjects consent, the following aspects should be considered:

- The Controllers has the ***burden of proving*** that he has received the consent for the processing (Article 7.1)
- If consent is issued in the context of a written statement on a different matter, it must have ***separate evidence*** from the rest of the document (Article 7.2)
- The ***revocation*** of the consent may take place at any time without prejudice to the legitimacy of the previous processing (Article 7.3).

In those circumstances in which there is no free choice by the data subject, in providing or revoking the consent, this is understood as not free; in such cases the consent loses its function as a prerequisite of lawfulness [Recital 42 and Article 7.4].

RIGHTS OF DATA SUBJECTS

The rights of the data subjects constitute the first pendant of the the legislation on the protection of personal data, followed by the supervisory authority powers, administrative and judicial protection and the sanction system.

Regulation 2016/679 transposes the overall system of Directive 95/46/EC on the rights granted to data subjects.

The subjects to which the information refers (the so-called "data subjects") see the basket of their rights expanded: in addition to those already known of ***access, integration, rectification, restriction***, new rights are also added. These are the right to be forgotten and the portability right.

Violation of any of the rights of data subjects is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

Access Right

Regulation 2016/679 refers to access as a general right of the data subject to acquire information: not only to be informed about the personal data concerning him, subject to processing by the Controller, but also to obtain (upon request) additional information for a correct and complete transparency regarding the same processing (Article 15).

If, therefore, the notice can be considered as the effect of the right of the data subject to be informed, access is the manifestation of his right to inquire about the following profiles, in fact corresponding to the contents of the notice:

- the ***purpose*** of the processing;
- the ***categories of processed personal data***;
- ***recipients or categories*** of recipients to whom personal data are communicated;
- the ***retention period*** for the personal data or, if not possible, the criteria used to determine it;
- the existence of the ***right*** to request the rectification or deletion of the data concerning him or the limitation of the processing or to object to their processing;
- the right to lodge a ***complaint*** with the supervisory authority;
- the ***source*** of the acquisition, if the data is not collected directly from the data subject;
- the existence of ***automated decision-making processes***, including ***profiling*** and significant information on the logic used, as well as the importance and consequences for the data subject;

in case of ***transfer of data beyond EU territories***, the existence of adequate security measures.

Right to Rectification

The right to rectification is contained in Section 3 of the GDPR. The related article is Art. 16 and it reads as follows:

> "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

This right requires the adoption of appropriate measures for the rectification of the personal data of the data subject, with the obligation to inform, where possible, any third party to which the data has been transmitted. It is therefore evident how important the control of the supply chain is, together with an appropriate census of all existing transfers of personal data to third parties.

Right to Erasure

The data subject shall have the right to obtain from the Controller the erasure of his/her personal data in the following cases:

- when it is no longer needed in relation to the purpose of collection [art. 17.1, a)]
- when the consent has been withdrawn [art. 17.1, b)]
- when the data subject objects to the processing [art. 17.1, c)]
- when the data are unlawfully processed [art. 17.1, d)]
- when the erasure derives from a legal obligation [art. 17.1, e)]
- when the data was collected for the provision of an information society service in favor of a minor and with his consent [art. 17.1, f)].

Right to be Forgotten

The right to erase personal data on the internet (right to be forgotten) is conceived as a declination of the general right of erasure (Article 17.2).

The GDPR provides that if the data controller has «made the personal data public and is obliged (…) to erase the personal data», in accordance with the provisions of Article 17.1, he must «inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data».

This obligation must be executed "taking account of available technology and the cost of implementation" and adopting "reasonable steps, including technical measures".

Right to be Forgotten: History

The right to be forgotten had already caused a stir during the validity of Directive 95/46/EC because it was recognized as already existing by the ECJ in the well-known Google case. A prerogative, this, which especially concerns the internet user

in order to counter the phenomenon of fossilization of information in the web timeless space.

The ECJ has found it unlawful that events that have long since passed can continue to be offered to the internet reader as news of the day, even though they are decontestualized and no longer topical; Regulation 2016/679 now provides precise regulatory support without the need for interpretative reconstructions through the provision contained in art. 17.

Right to Restriction of Processing

In some circumstances, the data subject has the right to obtain a restriction of the processing (Article 18).

The cases of exercise of the right to restriction of processing are when one of the following applies:

- the data subject contests the accuracy of the personal data, for the period required to verify the data accuracy [art. 18.1, a)];
- the processing is unlawful and the data subject opposes the erasure and asks for restriction as an alternative [art. 18.1, b)];
- with the processing ceased, the data subject needs the data to exercise his/her own right to trial [art. 18.1, c)];
- the data subject has objected the processing for legitimate reasons, pending the necessary verifications [art. 18.1, d)].

Portability Right

Of particular importance is the new right to portability (Article 20) which gives the data subject the power to obtain his/her personal data from the Controller in an "open" format, easily usable on the most widely used platforms: another "bridge" launched between the world of data protection and the increasingly contiguous one of the competition.

Where the legal basis of the processing is given by the consent or execution of a contract and the processing is carried out by automated means, the right to portability includes the right of the data subject to obtain the direct transmission of his personal data from one Controller to the other, if technically feasible (Article 20.2).

Free Exercise of Rights

The exercise of all data protection rights is normally free, both for the information provided and for the actions taken (Article 12.5).

Exception is the case where «requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character», in which case the Controller may charge a reasonable fee on the administrative costs incurred or refuse to process the request. In such a case, the burden of proof of the manifestly disproportionate nature of the claim is on the Controller.

If, in general, the Controller refuses to comply with the requests of the data subject, he must inform him of the reasons and the possibility for the data subject to file a

complaint with the National Supervisory Authority and to apply to the ordinary judicial authority (Article 12.4) .

Right to Object

Where the processing is necessary for the execution of a public interest task or for the pursuit of a legitimate interest of the data controller or a third party, the data subject has the right to object to the processing of his/her personal data in the presence of legitimate reasons related to his/her particular circumstances.

As already provided in Directive 95/46/EC, the objection to the use of personal data for direct marketing purposes is fully discretionary (Article 21.2).

GDPR DOCUMENTATION SYSTEM

The Regulation changes the axe for the legitimacy of the processing of personal data, moving it from the so-called legitimacy requirements1 to the compliance data protection system and the direct attribution of responsibility to the data controller.

In summary, the Regulation stipulates that compliance with the obligations of the data controller – for whose satisfaction he is therefore responsible and he is required to demonstrate it – can be expressed as follows:

- through a documentation system consisting in the maintenance of the record of processing activities, descriptive of the processing carried out under its own responsibility (Article 30) and further compulsory documentation
- the adoption of appropriate policies (Article 24) and compliance assessments with regard to processing and effectiveness assessments concerning the data protection measures implemented
- adherence to approved Code of Conducts (Articles 24.3, 28.5, 32.3)
- the use of a certification mechanism (Articles 24.3, 25.3, 28.5, 32.3).

Therefore, documentation requirements, assessments and compliance with codes of conduct and data protection certification systems are tools to demonstrate compliance of the company with legal requirements.

Records of Processing

The obligation of documentation has its core in the register of processing (Article 30).

Specifically, the document must contain the following information:

- contact data of the Data Controller, eventual joint-controllers, national representatives and data protection officer [art. 30.1, lett. a)];
- purpose of the processing [art. 30.1, lett. b)]
- categories of data subjects and the categories of data referred to them [art. 30.1, lett. c)]
- categories of recipients to whom data are transmitted (including recipients in third countries) [art. 30.1, ch. d)]
- third countries to which personal data and related processing operations are transmitted together with the documentation of the appropriate security measures when the transfer is based on the legitimate interests of the data controller [art. 30.1, lett. e)]
- where possible, retention periods for the different categories of data used [art. 30.1, lett. f)]
- where possible, a general description of the adopted technical and organizational security measures [art. 30.1, lett. g)].

This documentation, which should also be prepared by the Processor (Article 30.2), must be submitted to the National Supervisory Authority, upon request (Article 30.4).

Supporting Documentation

The system documentation is completed by the following "supporting documentation", for which GDPR requires the conservation and management:

- Documentation on the relationship between "joint-controllers" (Article 26)
- Contractual determination of the relationship between Controller and Processor and related obligations (Article 28.3)
- Violation of Personal Data, i.e. data breaches (Article 33.5)
- Appropriate assessments and guarantees regarding foreign data transfers based on the legitimate interest pursued by Controller or Processor (Article 49.6)1.

1. In a version of the proposed Regulation prior to that published on 21/1/2012, supporting documentation for foreign data transfers was also required, based on standard data protection clauses or binding corporate rules (Article 39.3).

Abolition Obligation Notification

The obligation to maintain the system documentation under the responsibility of the data controller replaces the previous obligation to notify the Authority laid down in the Directive 1.

1. See Section IX, Articles 18 and subsequents, Dir. 95/46/EC.

Sanction for Violation of Documentation

The vioaltion of obligations regarding proper management and retention:

- of the register of processing activities
- of supporting documentation regarding any breaches of personal data and assessments of foreign data transfers made on the basis of the legitimate interest of the Controller

is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Prior Consultation to Supervisory Authority

The Controller must consult the national supervisory authority prior to processing, if the impact assessment referred to in Article 35 reveals that the processing itself would pose a high risk in the absence of proper measures adopted by the Controller to mitigate the risk (Article 36).

Sanction for Omitted Prior Consultation

Violation of the prior consultation obligation is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.4).

DATA PROTECTION ASSESSMENT

When a data processing poses specific risks, it is subject to a preliminary impact assessments (DPIA).

DPIA

When it is likely that the processing, by its nature, its object or purposes, entails "high risks to the rights and freedoms" of the data subject, the data controller will have to carry out an ex ante evaluation of the impact that the processing may have from a data protection perspective: this is the so called Data Protection Impact Assessment (DPIA). The obligation laid down in Article 35 constitutes the manifestation of the accountability of the Controller (Articles 5.2 and 24) where, by means of a prior assessment, specific risks to the rights of the data subjects are encountered, caused by the usage of «new technologies, and taking into account the nature, scope, context and purposes of the processing».

Sanction for Omitted DPIA

Violation of the obligation for the Controller to carry out the data protection impact assessment (DPIA) is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Supervisory Authority Consultation

Regulation 2016/679 has given mandate to the individual national authority to identify the types of processing that require to carry out such an assessment (Article 35.4).

TECHNICAL AND ORGANIZATIONAL MEASURES

Security Measures

Security is in itself a micro-system within the broader data protection scenario (Article 32). Technical and organizational measures play a fundamental role according to the Regulation, at least under six distinct profiles:

- They determine the level of security adopted (Article 32)
- They must allow the Controller to adequately protect the data from any breach (Article 33) and to allow it to react promptly in the event of a breach
- They must be able to adequately support the exercise of the data subjects' rights (eg Article 17.2)
- They must be able to reduce the risks associated with the protection of personal data [eg. art. 22.2, b)]
- Depending on their type and quality, they affect the risk assessment
- They constitute an important organizational criterion in the management of controllers, agents, subcontractors (eg articles 24.1, 28.1, 28.4)
- They allow verification and demonstrate the accountability level of the Controller [eg Art. 25.1, 30.1 g), 30.2 d)].

Failure to take appropriate security measures is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Security in General

Regardless of Italian legislation (Dlgs 196/2003), the GDPR does not require specific security measures, albeit minimal, but imposes a generic obligation on both the Controller and the Processor, to take measures to mitigate the risks associated with the data processing (Article 32). This, as stated below, involves the requirement for an initial assessment of adequacy between risks and measures for the Company; since the measures taken must ensure an appropriate level of security, given the state of the technology and the related costs.

The provision of Article 32 concerns, in addition to "technical" measures, those of an organizational nature; both must be the result of a risk analysis.

Security Assessment

Determining the measures to be taken requires a complex evaluation process.

The estimate of their adequacy must be based on the analysis «the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons» (art. 32.1).

In addition, the risks to be assessed are those presented by «accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed» (art. 32.2).

According to the principle of accountability (Article 24), the Controller must take into account the validity of his assessments.

DATA BREACH

Security Measures against Data Breaches

The organizational and technical measures mentioned in the Regulation are the cornerstone of the discipline: they concern both the most appropriately technical measures (such as authentication credentials, authorization profiling system, encryption, antivirus and back up etc.) and the organizational ones (such as contractual regulation of relationships with those data processors, confidentiality constraints and instructions given to individuals who work on data, policies and records of processing, etc.). One of the interaction profiles of organizational and technical measures with the security system is to protect and respond to personal data breaches.

The declination of organizational and technical measures in the information security system

Technical-organizational measures interact with the entire system for the protection of personal data under different profiles:

- As a system of protection and reaction to violations (data breach)
- As verification and demonstration of compliance (accountability)
- As a tool for reducing risk (minimizing data, pseudonymization, privacy by design)
- As a Risk Assessment Component (DPIA)
- As organizational measure (contractual constraints with processors, confidentiality of people managing data, policies and registers)
- As a way of faacilitating the exercise of rights (opposition, forgiveness or cancellation, limitation of processing, portability, profiling and automated decisions).

Prevention and reaction to data breaches

The security measures objectives – found in the Regulation – are dual:

- of an "active" or a preventative nature, consisting in reducing the risk of unauthorized destruction, loss, modification, disclosure or accidental or unlawful access to personal data
- of a "passive" or "reactive" nature, consisting in a prompt response to incidents in the implementation of effective remediation actions and timely communications to the competent authorities, data subjects and the Controller (if the incident concerns the Processor).

The criterion of adequacy of the measures

The "active" protection profile requires the adoption of an adequate security level. The determination of the adequacy of the level is achieved adopting a risk-based approach: «appropriate technical and organisational measures to ensure a level of

security appropriate to the risk» should be implemented, «taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons» (Article 32 (1)).

The legislator provides an example list of such measures that may include:

- «(a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.».

Data breach incidents

On the "reactive" front, in addition to system resilience and recovery policies, the legislator imposes specific disciplines in case of data breaches.

The state of the law

It should be noted that, according to EU Regulation no. 611/2013, concerning publicly available electronic communications providers, encryption or hashing systems are not considered to be comprehensive remedies for protection against the risk of infringement, as they must be accompanied by appropriate organizational and technical measures under art . 17 of Directive 95/46 [Recital (17)]. However, they allow – if they comply with the conditions laid down – to avoid notifying users in case of a breach (see Article 4).

Cybersecurity Directive

The so-called Cybersecurity Directive is being published on the Official Journal of the European Union. The Directive envisages for energy, transport, banking, financial market infrastructure, health and water supply services:

- the adoption of security measures to manage the risks to the networks and information systems that they control and use in their respective activities
- the notification to the competent authorities of those incidents having a significant impact on the continuity of the essential services they provide.
- These provisions should be harmonized with the corresponding ones contained in the Regulation on the processing of personal data.

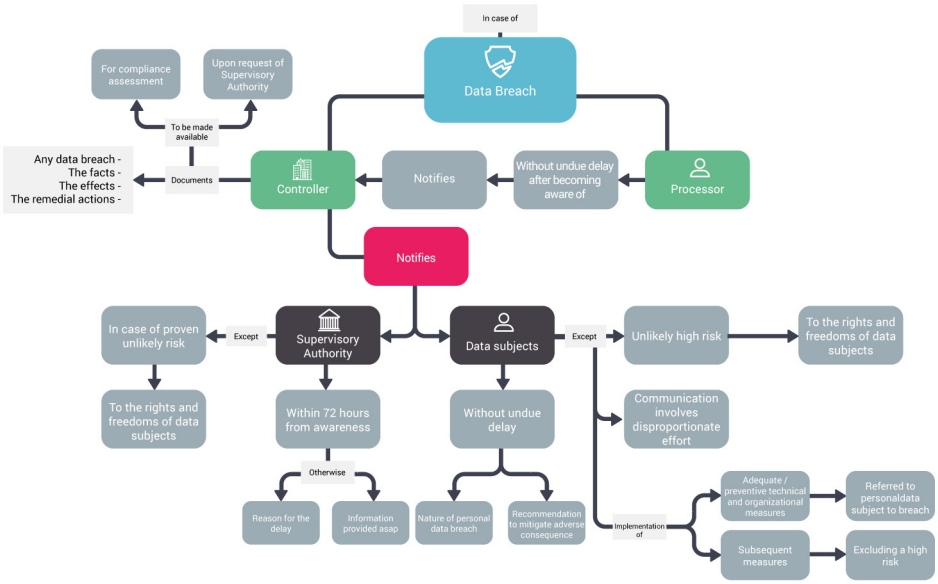
GDPR

The Regulation extends the reporting obligations for personal data breaches to their respective competent authorities, to all Data Controllers. The notification must be made without unjustified delay and, in any case, within 72 hours of the date on which it has become known, unless the Controller demonstrates that it is unlikely that the data breach would present a risk to the rights and freedoms of the data subjects affected by the breach. If the notification takes place after the 72-hours

deadline, the reasons for the delay must be explained [Recital (67) and art. 31]. In the event of a high risk for the rights and freedoms of the data subjects, notification should also be made to the latter, by making recommendations to mitigate potential adverse effects. Notification to data subjects must be carried out «as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities» [Recital (86)].

Adopting appropriate technical measures to effectively limit the risk of identity theft or other forms of abuse positively affects the consequences of a data breach and the resulting legal implications.

Personal Data Breach



Personal Data Breach
Regulation (EU) n.2016/679

Sanction for Sensitive Data Breach

Infringement related to the processing of sensitive data (Article 9) is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

DATA TRANSFER ABROAD

The flow of personal data

- from a country belonging to the European Union or the European Economic Area (EEA, ie outside the territories of all EU Member States beyond Norway, Iceland and Liechtenstein)
- to another country

is subject to specific rules to ensure that the protection granted to personal data under European law is not affected by transferring the same data to a country without a system of safeguards considered similar to that guaranteed in the EU.

1.1. Countries that offer personal data protection system, considered appropriate by the EU Commission

The external flow of personal data between

- a country of the European Economic Area (or EEA) and
- an extra-EU country

is considered legitimate and free if the European Commission has previously recognized with its own formal decision that there is a data protection system at the receiving country which offers personal data a protection similar to what they enjoy under EU law.

1.2. Countries not on the list of those with "adequate protection"

In the event that the receiving country is not included in the list of data protection adequate countries, a legal ground must be identified that makes such transfer legitimate. One of these legitimacy conditions that can be used effectively in transactions concerning the Company's relationship with Third Parties is the use of contractual terms binding the Company and the receiving Third Party to the same guarantees as provided by EU law for the protection of personal data. In this way, the obstacle to the non-applicability of EU law to the non-EU third-party is overcome, binding the Third Party to contractual requirements comparable with the rules set forth by the law.

For this legitimacy requirement to go beyond the ban on the transfer of personal data to countries without adequate protection, the contractual clauses used must be exactly the same as those officially approved by the EU Commission without any modifications.

1.3. The various contractual models approved by the EU Comission

In this respect, the Commission has, over the years, approved several sets of standard contractual clauses dealing with the following cases:

- Personal data flows between the EU Controller (the data exporter) and the Extra-EU Controller (the data importer)
- Personal data flows between the EU Controller (the data exporter) and the Extra-EU Processor (the data importer)
- Personal data flows between Data Processor and Data Processor.

SANCTIONS AND DAMAGES

New Sanctions

The extent of administrative sanctions (up to 4% of the total annual turnover – Article 83) suggests revising the data protection risk assessment approach, in order to update it and adjust the risks determination.

Sanction for Sensitive Data Breaches

Infringement related to the processing of sensitive data (Article 9) is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

Sanction for Omitted Prior Consultation

Violation of the prior consultation obligation is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.4).

Sanction for Omitted DPIA

Violation of the obligation for the Controller to carry out the data protection impact assessment (DPIA) is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Sanction for Consent Violations

Violation of the obligations regarding consent and its requirements as a prerequisite of lawfulness (Articles 6, 7 and 9) is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

Sanction for Rights Violations

Violation of any of the rights of data subjects is sanctioned with administrative fines of «up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.5).

GDPR-RELATED DEFINITIONS

Binding Corporate Rules (BCRs) - a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation)

Biometric Data - any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification

Consent - freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Concerning Health - any personal data related to the physical or mental health of an individual or the provision of health services to them

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject - a natural person whose personal data is processed by a controller or processor

Delegated Acts - non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity

Derogation - an exemption from a law

Directive - a legislative act that sets out a goal that all EU countries must achieve through their own national laws

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Enterprise - any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

Filing System - any specific set of personal data that is accessible according to specific criteria, or able to be queried

Genetic Data - data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual

Group of Undertakings - a controlling undertaking and its controlled undertakings

Main Establishment - the place within the Union that the main decisions surrounding data processing are made; with regard to the processor

Personal Data - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution

Recipient - entity to which the personal data are disclosed

Regulation - a binding legislative act that must be applied in its entirety across the Union

Representative - any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities

Right to be Forgotten - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Supervisory Authority - a public authority which is established by a member state in accordance with article 46

Trilogues - informal negotiations between the European Commission, the European Parliament, and the Council of the European Union usually held following the first readings of proposed legislation in order to more quickly agree to a compromise text to be adopted.