

# **HOPEX GDPR**

## **User Guide**



HOPEX V2R1

Information in this document is subject to change and does not represent a commitment on the part of MEGA International.

No part of this document is to be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the prior written permission of MEGA International.

© MEGA International, Paris, 1996 - 2018

All rights reserved.

HOPEX GDPR is a registered trademarks of MEGA International.

Windows is a registered trademark of Microsoft Corporation.

The other trademarks mentioned in this document belong to their respective owners.

# CONTENTS



---

<b>Introduction to HOPEX GDPR</b>	<b>7</b>
<b>About the GDPR</b>	<b>8</b>
What is GDPR ?	8
What is personal data?	8
<b>Pre-Requisites to Using HOPEX GDPR</b>	<b>9</b>
<b>Connecting to HOPEX GDPR</b>	<b>10</b>
<b>Profiles used in HOPEX GDPR</b>	<b>11</b>
Summary of HOPEX GDPR Profiles	11
Detailed Rights for Main HOPEX GDPR Profiles	12
<b>Learning material and Templates</b>	<b>14</b>
<b>Useful Features</b>	<b>15</b>
<i>Displaying the properties window on a permanent basis</i>	15
<i>Object status</i>	15
<i>Collaboration features</i>	15
<i>The search features</i>	15

---

<b>Setting Up the HOPEX GDPR Environment</b>	<b>17</b>
<b>Accessing the HOPEX GDPR Environment</b>	<b>18</b>
<b>Defining Data categories</b>	<b>19</b>
<b>Defining Data Subject Categories</b>	<b>21</b>
<b>Defining Sensitive Activities</b>	<b>22</b>
<b>Defining Transfer Safeguards</b>	<b>23</b>
<b>Defining Supervisory Authorities</b>	<b>24</b>
<b>Defining Country Adequacy</b>	<b>25</b>
<i>About Country adequacy</i>	25
<i>Accessing country-adequacy information</i>	25
<i>Country-adequacy information use in HOPEX GDPR</i>	25

<b>Defining Security Measures</b> . . . . .	<b>26</b>
<b>Defining Technologies</b> . . . . .	<b>27</b>
<i>Computing devices</i> . . . . .	27
<i>Removable devices</i> . . . . .	27
<b>Defining Physical Archives</b> . . . . .	<b>28</b>

---

## **Defining the Organization . . . . . 29**

<b>Creating Legal Entities and Departments</b> . . . . .	<b>30</b>
<i>Introduction to Entities and Departments</i> . . . . .	30
<i>Creating a Legal Entity</i> . . . . .	30
<i>Creating Departments</i> . . . . .	30
<i>Populating Legal Entities and Departments</i> . . . . .	30
<b>Defining Legal Entity Properties</b> . . . . .	<b>32</b>
<i>General properties of entities</i> . . . . .	32
<i>Managing establishments</i> . . . . .	32
<i>Managing national representatives</i> . . . . .	32
<i>Managing contractual agreements</i> . . . . .	33
<i>Managing users</i> . . . . .	33
<b>Managing Departments</b> . . . . .	<b>35</b>
<i>Defining Department Main Characteristics</i> . . . . .	35
<i>Connecting Users to a Department</i> . . . . .	35
<i>Defining Establishments</i> . . . . .	35
<i>Creating an establishment</i> . . . . .	36
<i>Specifying the HQ establishment for an entity</i> . . . . .	36
<i>Specifying the country of a legal entity</i> . . . . .	36
<b>Defining an Organizational Model</b> . . . . .	<b>38</b>
<b>Managing Third Parties</b> . . . . .	<b>39</b>
<b>Viewing the DPO Organizational Chart</b> . . . . .	<b>40</b>
<b>Managing Company Guidelines</b> . . . . .	<b>41</b>
<i>Creating company guidelines</i> . . . . .	41
<i>Attaching company guidelines information</i> . . . . .	41
<i>Assessing company guidelines</i> . . . . .	41
<b>Converting HOPEX EA Org-Units to Organizations</b> . . . . .	<b>42</b>
<i>Converting Org-Units to Organizations</i> . . . . .	42
<i>Synchronizing EA-GDPR organization</i> . . . . .	42

---

## **Describing Processing Activities in HOPEX GDPR . . . . . 43**

<b>Presentation of Processing Activities</b> . . . . .	<b>44</b>
<b>Pre-requisites to Processing Activity Creation</b> . . . . .	<b>45</b>
<b>Creating Processing Activities</b> . . . . .	<b>46</b>
<i>Creating Processing Activities from HOPEX Objects</i> . . . . .	46
<i>Importing data from HOPEX</i> . . . . .	46
<i>Creating processing activities from processes</i> . . . . .	46

Creating processing elements from applications . . . . .	47
Creating Processing Activities in HOPEX GDPR . . . . .	47
<b>Accessing the Records of Processing . . . . .</b>	<b>48</b>
Accessing Processing Activities . . . . .	48
Refining the Scope of the Records of Processing . . . . .	48
<b>Describing Processing Activities. . . . .</b>	<b>50</b>
Processing Activity Dashboard . . . . .	51
Processing Activities Overview . . . . .	52
Additional information to specify . . . . .	52
Information in read-only mode . . . . .	53
Scope of the processing activity . . . . .	53
Computed information . . . . .	54
Processing Activities Legal Basis . . . . .	54
<b>Processing Activity Details . . . . .</b>	<b>56</b>
Processing Activities Levels of Detail. . . . .	56
Processed Personal Data . . . . .	57
Qualifying Minimization. . . . .	57
Viewing the computed risk . . . . .	58
Specifying the retention period on a processing activity . . . . .	58
Data Subject Right and Notice Management . . . . .	58
Specifying data subject rights for a processing activity. . . . .	60
Viewing data subject rights for all your processing activities . . . . .	60
Giving a compliance score for data subject rights . . . . .	60
Data Transfers . . . . .	61
Specifying data transfers on a processing activity . . . . .	61
Giving a compliance score for transfers . . . . .	61
Security Measures . . . . .	62
Specifying security measures on a processing activity . . . . .	62
Giving a compliance score for security measures . . . . .	62
Technologies and Physical Archives . . . . .	62
Contractual Agreements and Other Attachments . . . . .	63
<b>Managing Processing Activity Elements . . . . .</b>	<b>64</b>
Creating a processing element . . . . .	64
Specifying an application processing element . . . . .	65
Displaying the application properties and web site . . . . .	66
<b>Using the Processing Activity Workflow. . . . .</b>	<b>67</b>
Asking the activity owner to complete processing activity description. . . . .	67
Submitting processing activity description . . . . .	68
Submitting pre-assessments and DPIAs . . . . .	68
<b>Processing-Related Reports . . . . .</b>	<b>69</b>
Accessing Processing-Related Reports . . . . .	69
Records of processing . . . . .	69
About the record of processing . . . . .	69
Creating a record of processing . . . . .	70
Cross-border transfer map . . . . .	70
Pre-requisites to using cross-border transfer map . . . . .	71
Content of the transfer map . . . . .	71
Additional information about transfers . . . . .	71
CNIL-Specific Report . . . . .	72
Activating the CNIL Report . . . . .	72
Prerequisites for the CNIL report . . . . .	72

Generating the CNIL report . . . . .	72
--------------------------------------	----

---

## **Assessing Processing Activities . . . . . 73**

### **Prerequisites to Processing Activity Assessment . . . . .74**

Specifying Compliance Levels . . . . .	74
<i>Legal Basis Compliance Level</i> . . . . .	74
<i>Minimization Compliance Level</i> . . . . .	75
<i>Data transfers and security measures</i> . . . . .	75
Viewing the Initial Compliance Level of a Processing Activity . . . . .	75

### **Performing a Pre-assessment. . . . .77**

Consulting Decision-Making Reports . . . . .	77
<i>Accessing your dashboard</i> . . . . .	77
<i>Processing activities by compliance level</i> . . . . .	77
<i>Processing activities by assessment status (DPIA)</i> . . . . .	78
<i>Processing activities by risk scale</i> . . . . .	79
Performing the Pre-Assessment . . . . .	79
Consulting the History of Pre-assessments . . . . .	80

### **Performing Impact Assessment (DPIA) . . . . .82**

About DPIAs. . . . .	82
<i>When to conduct a DPIA?</i> . . . . .	82
<i>What is a DPIA?</i> . . . . .	82
Creating a DPIA . . . . .	82
<i>Starting a DPIA from scratch</i> . . . . .	82
<i>Reusing a DPIA</i> . . . . .	82
<i>Editing a DPIA</i> . . . . .	83
Assessing Risks . . . . .	83
Defining Recommendations and Remediation Actions . . . . .	85
Attaching Documents to the DPIA . . . . .	85
Validating the DPIA. . . . .	85
<i>Final risk level</i> . . . . .	86
<i>Final compliance level</i> . . . . .	86
<i>Subsequent Action</i> . . . . .	86
Consulting DPIA Reports and Results. . . . .	86
<i>Viewing the dashboard of the processing activity</i> . . . . .	86
<i>Record of DPIAs</i> . . . . .	87
<i>Generating a DPIA document</i> . . . . .	87

---

## **Managing Data Breaches. . . . . 89**

Declaring a Data Breach . . . . .	89
Specifying Data Breach Scope . . . . .	91
Assessing a Data Breach . . . . .	91
Planning Remediation actions . . . . .	92
Notifying a Data Breach . . . . .	92
Viewing Elapsed Time since Breach Discovery . . . . .	92

Duplicating Data Breaches .....	93
---------------------------------	----

---

## **Managing Data Subject Requests ..... 95**

Creating a data subject request .....	95
Specifying Information on a Data Subject Request .....	97
Describing the scope of a data subject request .....	97
Attaching documents to the data subject request .....	98
Managing data subject management deadlines .....	98

---

## **Demonstrating Compliance ..... 99**

Processing Activity Status .....	99
Legal Basis .....	100
Sensitive Activities .....	101
Record of DPIAs .....	101
Data Risk Report .....	102
Data Transfers .....	103
Data Subject Rights Report .....	103
Third-Parties Report .....	103
<i>Pre-requisites</i> .....	104
<i>Launching the Third-party report</i> .....	104
<i>Third-party report content</i> .....	104
Record of Processing .....	105
Cross-border transfer map .....	105
IT Applications .....	105
Notice .....	106
Data Breaches .....	107

---

## **FAQs ..... 109**

About Processing Activities .....	109
About Assessments .....	110
About Transfers .....	111
About HOPEX GDPR Import and HOPEX Integration .....	112
Miscellaneous .....	113

## **GDPR Glossary ..... 115**





# INTRODUCTION TO HOPEX GDPR



**HOPEX GDPR** is a SaaS solution which helps you manage your compliance to the GDPR (General Data Protection Regulation).

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.

The methodology has been developed with Gruppo IMPERIALI, who brings more than 30 years of Data Protection legal expertise. **HOPEX GDPR** integrates up-to-date regulatory details and legal templates to accelerate your remediation plans.

**HOPEX GDPR** enables you to reuse processes and applications created in **HOPEX Business Process Analysis**, **HOPEX IT Architecture** and **HOPEX IT Portfolio Management**.

# ABOUT THE GDPR

---

## What is GDPR ?

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.

---

## 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.*

## PRE-REQUISITES TO USING HOPEX GDPR

The first time you install **HOPEX GDPR** you need to import a specific solution pack to each data repository.








☛ *The Solution Pack GDPR.exe that you need to import needs to be decompressed (HOPEX installation folder > Utilities > Solution Pack, double-click the Solution Pack to extract it).*

To import the Solution Pack:

1. From **HOPEX Administration**, connect to the environment concerned.
2. Expand the **Repositories** folder.
3. Right-click the repository and select **Object Management > Import Solution Pack**.  
The Solution Pack Import dialog box appears.
4. Select the Solution Pack "GDPR.exe".
5. Click **OK**.  
The Import MEGA Data XML dialog box displays import progress.  
The selected Solution Pack is imported into the repository.

# CONNECTING TO HOPEX GDPR

To connect to **HOPEX GDPR**:

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 GDPR](#).  
 *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 GDPR

### Summary of HOPEX GDPR Profiles

Profiles	Definition
GDPR Functional Administrator	The GDPR functional administrator is an individual who ensures that all information required is available to the experts. He has rights on all reference data (eg. data categories, security measures). He is responsible for defining the environment.
Activity owner	The 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.
Application owner	The application owner provides a detailed description of IT applications used in the context of a processing activity. This profile is similar to Activity Owner but at the application level.
DPO	The DPO plays the role of advisor in the company, GDPR compliance correspondent to the regulatory authority and first point of contact for data subjects' claims. The Data Protection Officer (DPO) works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR. He 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 GDPR 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.
DPO correspondent	The DPO correspondent tasks are the same as the DPO but are restricted to a sub-set of the organization.
GDPR Team	The GDPR 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 who is responsible for the overall company compliance level to GDPR.

## Detailed Rights for Main HOPEX GDPR Profiles

Actions	Functional Administrator	Activity Owner/ Application Owner	Chief Privacy Officer	DPO/ DPO Deputy/ GDPR Team
<a href="#">Setting Up the HOPEX GDPR Environment</a> <b>(Key Elements</b> section) - Data categories - Data subject categories - Sensitive activities - Transfer safeguards - Supervisory authorities - Country adequacy - Security measures	X		X	
<a href="#">Defining the Organization</a> <b>(Organizaton</b> section) - Legal entities - Departments - Third parties - DPO Organizational chart - Company guidelines			X	
<a href="#">Describing Processing Activities in HOPEX GDPR</a> <b>(Record of Processing</b> section)		X	X	
<a href="#">Performing a Pre-assessment</a> <b>Record of Processing</b> section > <b>Pre-assessment</b> tab of a processing activity - Identifying compliance level - Identifying risk level			X	X

Actions	Functional Administrator	Activity Owner/ Application Owner	Chief Privacy Officer	DPO/ DPO Deputy/ GDPR Team
<a href="#">Performing Impact Assessment (DPIA)</a> <b>Record of Processing</b> section > <b>DPIA</b> tab of a processing activity - Defining Risks - Defining Recommendations and Remediation Actions			X	X
<a href="#">Managing Data Breaches</a> <b>Personal Data Breach</b> section			X	X
<a href="#">Managing Data Subject Requests</a> <b>Data subject Management</b> section			X	X

## LEARNING MATERIAL AND TEMPLATES

At all times you may access reference documentation about GDPR containing learning materials and templates.

To access the reference documentation page:

- 】 In each section of the navigation menu, select **Learning Material and Templates**, for instance from:
  - **Organization**
  - **Record of Processing**
  - **Incident Management**
  - **Reports**

The reference documentation contains:

- GDPR Documentation
  - Quick Guide
  - GDPR in details
- GDPR Templates
  - Contractual Templates
  - Data Privacy Templates
  - DPIA templates and instructions of use

☛ *You may use these templates suit your needs and attach them as business documents in **HOPEX GDPR** where appropriate.*

- GDPR SOP: Template for Standard Operating Procedures




# USEFUL FEATURES

☞ For more information on how to use the desktop and repository, see [Handling Repository Objects](#)

## Displaying the properties window on a permanent basis

You can choose to display the property windows in **HOPEX** on a permanent basis so as to view immediately the properties of an object.

To display the properties window on a permanent basis:

1. Click the **Details**  button on the top right-hand side.  
The **Properties** window appears in the Edit Area.
2. Select an object.  
Its properties appear.

## Object status

The objects of the environment have statuses in **HOPEX GDPR**.

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

- **candidate**: to be validated by a DPO / the GDPR team
- **live**: has been validated by the DPO / the GDPR 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 GDPR** simplifies teamwork and offers different means of communication. You can:

- create and participate in review notes on objects.
- add tags.  
☞ *Tags may be used with quick search to help you find a particular object. See [Quick Search \(Web Front-End\)](#).*
- view your activity.
- share with the other **HOPEX** users: add tags, like an object.  
☞ For more information, see [Communicating in HOPEX](#).

## The search features

**HOPEX GDPR** enables you to perform searches in the repository.

For more information, see [Searching Objects \(Web Front-End\)](#).



# SETTING UP THE HOPEX GDPR ENVIRONMENT



As a **GDPR functional administrator**, 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 GDPR** provides default data sets. It is necessary for you to analyze them in order to contextualize these sets to your company needs.

- ✓ [Accessing the HOPEX GDPR Environment](#)
- ✓ [Defining Data categories](#)
- ✓ [Defining Data Subject Categories](#)
- ✓ [Defining Sensitive Activities](#)
- ✓ [Defining Transfer Safeguards](#)
- ✓ [Defining Supervisory Authorities](#)
- ✓ [Defining Country Adequacy](#)
- ✓ [Defining Security Measures](#)
- ✓ [Defining Technologies](#)
- ✓ [Defining Physical Archives](#)

## ACCESSING THE HOPEX GDPR ENVIRONMENT

To view and modify key elements of your environment:

- In the navigation menu, click **Key Elements**.

The most important elements to be defined are:

- [Defining Data categories](#)
- [Defining Data Subject Categories](#).

Under GDPR key elements, you also have access to:

- [Defining Sensitive Activities](#)
- [Defining Transfer Safeguards](#)
- [Defining Supervisory Authorities](#)
- [Defining Security Measures](#)
- [Defining Country Adequacy](#) information

## DEFINING DATA CATEGORIES

In **HOPEX GDPR**, 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. In the navigation menu, click **Key elements > Data Categories**.
2. Identify the most common personal data categories used in your business processing activities.

List

Hierarchy View

New

<div><input type="checkbox"/></div>	Data Category Name ↑	Retention Period	Risk Scale	Description
<input type="checkbox"/>	Biometric	2 months	<div><div></div>High</div>	Data derived from somatic or behavioral char...
<input type="checkbox"/>	Contact	1 year	<div><div></div>Medium</div>	Data allowing direct identification, such as pe...
<input type="checkbox"/>	Cookies and System Logs	2 months	<div><div></div>Medium</div>	Data automatically generated when browsing ...
<input type="checkbox"/>	Financial	20 years	<div><div></div>High</div>	Financial data such as salary, bank account d...
<input type="checkbox"/>	Health	1 year	<div><div></div>High</div>	Data generated by devices or applications us...
<input type="checkbox"/>	Judicial	10 years	<div><div></div>High</div>	Data that may reveal the existence of certain j...
<input type="checkbox"/>	Sensitive	1 year	<div><div></div>High</div>	Data that can reveal racial and ethnic origin, r...

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 occur if data is lost, stolen or becomes unavailable.











- whether this data category corresponds to **Sensitive data**.

## DEFINING 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. In the navigation menu, click **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.

 New		
<input type="checkbox"/>	Data Subjects Category	Risk Scale ↑
<input type="checkbox"/>	Minors	 High
<input type="checkbox"/>	Customers	 Low
<input type="checkbox"/>	Shareholders	 Medium
<input type="checkbox"/>	Visitors	 Medium
<input type="checkbox"/>	Drivers	 Medium
<input type="checkbox"/>	Agents	 Medium
<input type="checkbox"/>	Employees	 Medium
<input type="checkbox"/>	Clients	 Medium
<input type="checkbox"/>	Suppliers	 Medium

# DEFINING SENSITIVE ACTIVITIES



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

To define sensitive activities:

- 1 In the navigation menu, click **Key elements > Sensitive activities**.

<div>New</div>			
<input type="checkbox"/>	Sensitive Activity ↑	Risk Scale	Description
<input type="checkbox"/>	Automated decision making with legal or similar significant effect	⚠ High	Processing that aims at taking de...
<input type="checkbox"/>	Automated processing of sensitive data	⚠ High	
<input type="checkbox"/>	Evaluation or scoring, including profiling and predicting	⚠ High	Especially from "aspects concerni...
<input type="checkbox"/>	Innovative use or application of new technological or organizational solutio...	⚠ High	Like combining use of finger print ...
<input type="checkbox"/>	Large scale systematic monitoring of publicly accessible areas	⚠ High	
<input type="checkbox"/>	Large-scale processing operations of sensitive data	⚠ High	
<input type="checkbox"/>	Matching or combining data sets	⚠ High	For example originating from two ...
<input type="checkbox"/>	Processing of data concerning vulnerable data subjects	⚠ High	The processing of this type of dat...
<input type="checkbox"/>	Processing of data on a large scale	⚠ High	The GDPR does not define what c...
<input type="checkbox"/>	Processing of sensitive data or data of a highly personal nature	⚠ High	This includes special categories o...

**HOPEX GDPR** 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:

- 1 In the navigation menu, click **Key elements > Transfer safeguards**.

+ New

<input type="checkbox"/>	Transfer SafeGuard ↑	Risk Mitigation	Description
<input type="checkbox"/>	Binding Corporate Rules (BCR)	 Very High	Binding Corporate Rules or "BCRs" were developed by the Europe...
<input type="checkbox"/>	Specific Consent	 Very High	The data subject can grant specific consent for the his/her perso...
<input type="checkbox"/>	Standard Contractual Clauses	 Very High	The European Commission can decide that standard contractual ...
<input type="checkbox"/>	US Privacy Shield	 Very High	The Privacy Shield is a framework for transatlantic exchanges of ...

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:

- 1 In the navigation menu, click **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	<b><i>Safeguards must be applied</i></b>

☛ For more information on safeguards, see [Defining Transfer Safeguards](#).

### Accessing country-adequacy information

To access country-adequacy information:

- 1 In the navigation menu, click **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 in HOPEX GDPR

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:

- 1 In the navigation menu, click **Key elements > Security Measures**.

Technical Measures			Certification Systems	Organizational measures
 New				
<input type="checkbox"/>	Name ↑	Security Measure Description		
<input type="checkbox"/>	Anonymization	Removal of personally identifiable information fro...		
<input type="checkbox"/>	Antivirus	Software used to prevent, detect and remove mali...		
<input type="checkbox"/>	Backup and Disaster recovery	Policies to backup data and restore it in case of di...		
<input type="checkbox"/>	Data Partitioning	Data partitioning is implemented in order to reduc...		
<input type="checkbox"/>	Encryption	Encoding of all data with techniques preventing un...		
<input type="checkbox"/>	Firewall	Network security system that monitors and contr...		
<input type="checkbox"/>	IDS	Intrusion detection system to detect unauthorized...		
<input type="checkbox"/>	Logging	Policies to define traceability and log management.		
<input type="checkbox"/>	Logical access control	Definition of different user profiles and authenticat...		

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

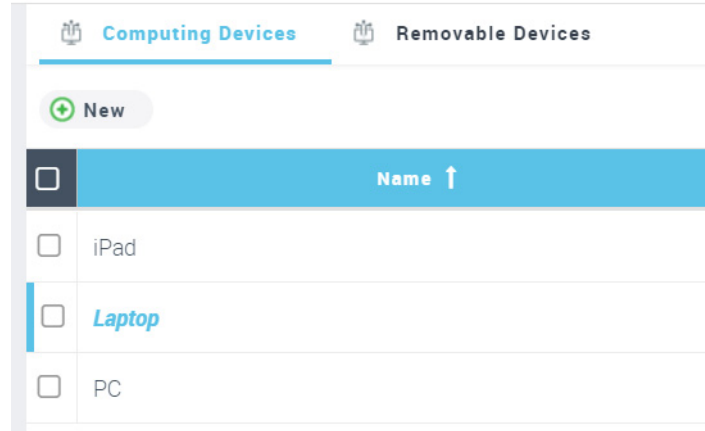
➡ *Security measures apply to data processing. Security measures which apply to transfers are called safeguards. For more details, see [Defining Transfer Safeguards](#).*

## DEFINING TECHNOLOGIES

To manage technologies:

- From the navigation menu, select **Key Elements > Technologies**.

You can add computing devices or removable devices.



### Computing devices

Un ordinateur est un matériel qui peut héberger et exécuter un logiciel.

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:

- 】 From the navigation menu, select **Key Elements > Physical Archives**.

Description of physical archives includes:

- Country
- Address
- Description

# DEFINING THE ORGANIZATION



As a functional administrator, you need to define the organization for the GDPR team members to be able to perform their duties.

To define the organization:

- In the navigation menu, click **Organization**.

You can create:

- legal entities
  - 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.*
- departments
  - See [Creating Legal Entities and Departments](#).
- third parties
  - See [Managing Third Parties](#).
- company guidelines
  - See [Managing Company Guidelines](#).
- the DPO organigram
  - See [Viewing the DPO Organizational Chart](#).

You can also convert HOPEX EA org-units to organizations to be used in HOPEX GDPR.

# 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.*

## Introduction to Entities and Departments

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

In **HOPEX GDPR**, 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. In the navigation menu, click **Organization > Legal entities & DPO**.
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. In the navigation menu, click **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. In the navigation menu of **HOPEX GDPR**, click **Organization > Legal entities & DPO**.
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 / GDPR team
- "Candidate": someone without the proper rights created the entity; it needs to be validated by the DPO or GDPR team
- "Obsolete": the entity no longer exists


 The Status is available for all main **HOPEX GDPR** concepts.

The property page offers more opportunities to describe legal entities.


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


 This piece of information depends on the country of the main establishment. If no establishment has been defined, the default value is "No".

## 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 GDPR.

To specify national representatives for an entity:

- 1. 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:


- 1. 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**
- **GDPR Specific clause**: 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.

 You may indicate if the agreement can be audited.

## Managing users

To assign users to a legal entity:

1. In the navigation menu, click **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.

☛ *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 GDPR**:

- 】 In the navigation menu select **Organization > Departments**.

In the property pages of a department, you can:

- specify general characteristics
  - ☛ See [Defining Department Main Characteristics](#).
- define the DPO et 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.
- **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 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. In the navigation menu, click **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. In the navigation menu, select **Organization > Legal Entities and DPOs**.
2. In the legal entity property page, select the **Establishments** tab.
3. Select the **HQ** check box.

Overview

Establishments

National Representatives

Specify all existing establishments of this legal entity.

New

	Name	HQ	Country
	Moscow Site	<input checked="" type="checkbox"/>	Russia
	Paris Site	<input type="checkbox"/>	France

## 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 GDPR compliance project.

To define your organizational model:

1. In the navigation menu, 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**

Business 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) works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.*
- Deputy DPO
  -  *A deputy DPO may assist the DPA 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 GDPR**:

- 1 In the navigation menu 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 GDPR**, 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:

- 1. In the navigation menu, select **Organization > DPO Organizational Chart**.

To define a DPO organizational chart if it is not already available:

1. In the navigation menu, 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 COMPANY GUIDELINES



*Company guidelines 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 company guidelines

To create company guidelines:

- In the navigation menu select **Organization > Policies & Procedures**.

You may provide the following information at company guideline creation:

- **Document name**
- **Scope:** legal entity or department concerned
- **Status:**
  - 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
  - Existing: the document is available
- **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 company guidelines information

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

- Select the **Attachments** tab of the company guideline created and attach a business document, or
- Select the **Link** tab of the company guideline and create an external reference indicating the relevant URL

## Assessing company guidelines

In the **Assessment** tab of the company guidelines, you may indicate the following:

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

# 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 GDPR**.

## Converting Org-Units to Organizations

To convert org-units to organizations:

1. From the navigation menu, click **Import > Organization**.
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 GDPR organization and the EA org-unit. The GDPR organization inherits from the org-unit local name, which becomes the legal entity/third party/department name.*

## Synchronizing EA-GDPR organization

When an object is modified in HOPEX, you can perform synchronization within **HOPEX GDPR**. 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 GDPR section, select "Displays synchronization buttons for GDPR-EA integration".

# DESCRIBING PROCESSING ACTIVITIES



- ✓ [Presentation of Processing Activities](#)
- ✓ [Pre-requisites to Processing Activity Creation](#)
- ✓ [Creating Processing Activities](#)
- ✓ [Describing Processing Activities](#)
- ✓ [Processing Activity Details](#)
- ✓ [Managing Processing Activity Elements](#)
- ✓ [Processing-Related Reports](#)

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

As a **GDPR 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 GDPR**.

You can also use processes and applications created in other **HOPEX** solutions to create the needed processing activities.

---

## Creating Processing Activities from HOPEX Objects

### Importing data from HOPEX

**HOPEX GDPR** enables you to import manually processes and applications.

To import objects from **HOPEX**:

1. From the navigation menu, select **Import > Import from HOPEX or Excel**.
2. Select the file you wish to import and click **OK** at the bottom of the page (on the right hand-side).

After data import the activity owner may create:

- processing activities from business/organizational processes.
- processing elements from applications

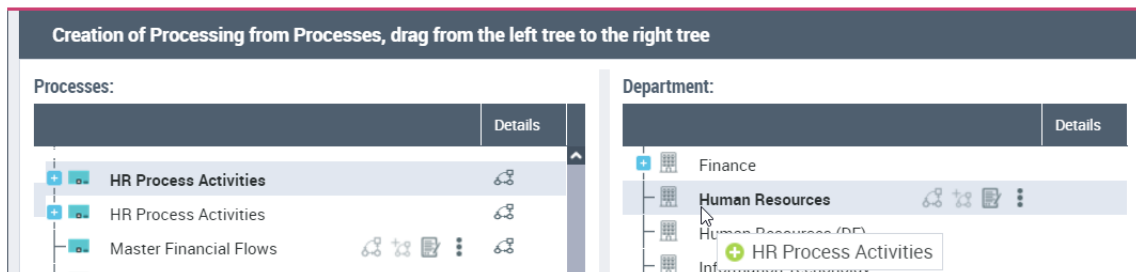
### Creating processing activities from processes

You can use a business or organizational process from other **HOPEX** solutions to create a processing activity.

To create a processing activity from a process:

1. From the navigation menu, select **Import > BPA Processes**.  
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 the Records of Processing](#).

☛ If you have troubles creating a processing activity from a sub-processing, you may find it useful to check our FAQs. See [About HOPEX GDPR Import and HOPEX Integration](#).

## Creating processing elements from applications

An **HOPEX** application can become a processing element in **HOPEX GDPR**.

☛ 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. From the navigation menu, select **Import > Import > ITPM/ITA 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. The processing element is automatically created under this processing activity.

## Creating Processing Activities in HOPEX GDPR

To create a processing activity directly in **HOPEX GDPR**:

1. In the navigation menu select **Record of Processing**.
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](#).



# ACCESSING THE RECORDS OF PROCESSING

## Accessing Processing Activities

To access processing activities in **HOPEX GDPR**:

1. In the navigation menu, select **Record of Processing**.
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

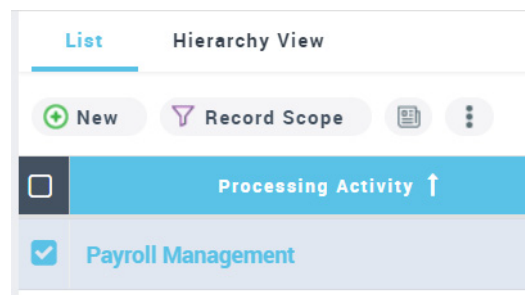
The GDPR requires to produce two separate records of processing activities:

- one as data controller
- one as data processor

**HOPEX GDPR** 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

As an activity owner, you have to describe processing activities in detail.

☛ For more information about processing activity creation, see [Creating Processing Activities](#).

☛ See also [Accessing Processing Activities](#).

As an activity owner, you need to use 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](#).

Payroll Management

Status: \* Live

**Overview** Legal Basis Details Preassessment DPIA

Processing Activity Purpose

Legal Entity \* HQ Entity

Main Department \* Organization-1

Data Protection Role Data Controller

Activity Owner Amy

☛ The **Pre-assessment** and **DPIA** tabs are to be used by the GDPR 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:

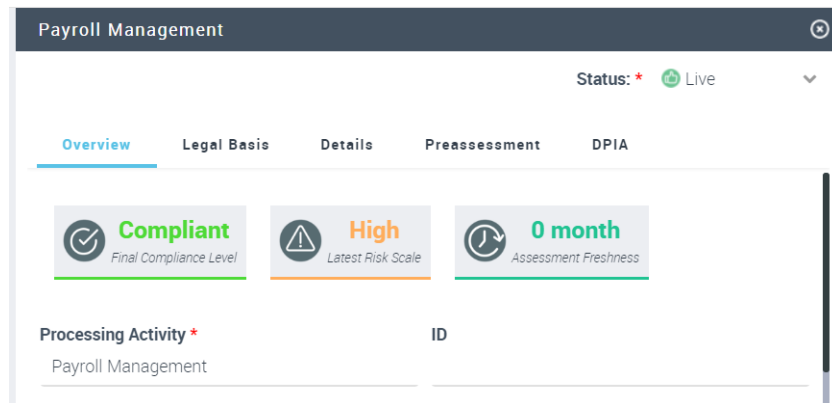


## Processing Activity Dashboard

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 GDPR team starts assessing the processing activity.

➡ For more information, see [Consulting DPIA Reports and Results](#).



## 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.*
- **Activity Owner**
  - 📖 *The activity owner provides a detailed description of the processing activity (excluding assessment).*
- **Details:** 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.

## Scope of the processing activity


To define the broad scope of a processing activity:





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

## 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 date: latest assessment performed
- the assessment status: indicates whether an assessment has been performed
- risk scale
- final compliance level

 If no assessments have been performed, the cell remains empty.


Creation Date	Assessment Date	Assessment Status	Risk Scale	Compliance Level
7/23/2018	7/23/2018	Done	 High	 Almost Compliant
7/23/2018	7/23/2018	Done	 Medium	 Almost Compliant
7/23/2018				

---

## 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.

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 six available lawful bases for processing. These are set out in Article 6 of the GDPR. 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 GDPR team can later assess the **Legal basis** based on the check boxes previously selected by the activity owner.



# PROCESSING ACTIVITY DETAILS

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

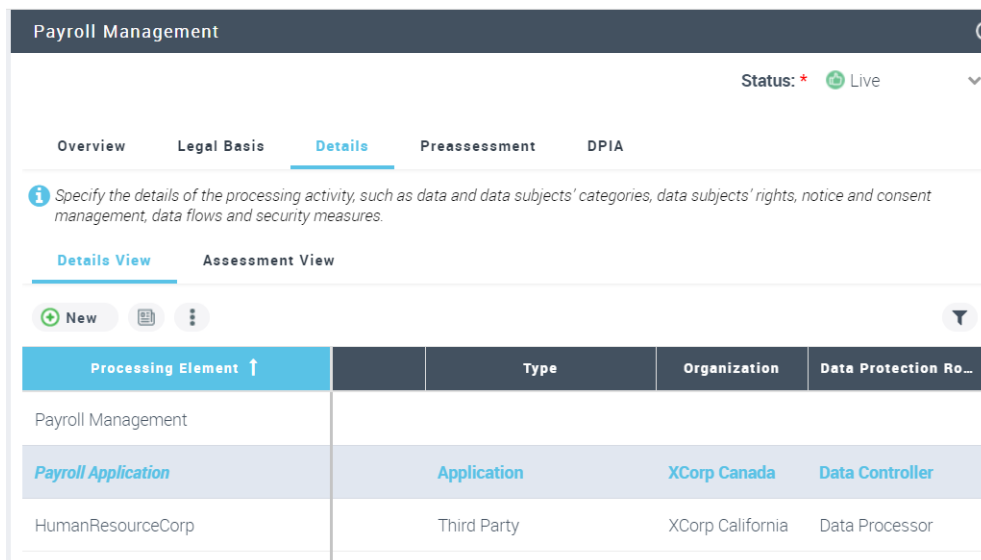
## Processing Activities Levels of Detail

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](#).



Payroll Management				
Status: * <span>Live</span>				
Overview	Legal Basis	Details	Preassessment	DPIA
<i>Specify the details of the processing activity, such as data and data subjects' categories, data subjects' rights, notice and consent management, data flows and security measures.</i>				
Details View Assessment View				
New [icon] [icon]				
Processing Element ↑	Type	Organization	Data Protection Ro...	
Payroll Management				
Payroll Application	Application	XCorp Canada	Data Controller	
HumanResourceCorp	Third Party	XCorp California	Data Processor	

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

- [Processed Personal Data](#)
- [Data Subject Right and Notice Management](#)
- [Data Transfers](#)
- [Contractual Agreements and Other Attachments](#)

## Processed Personal Data

To create processed personal data in **HOPEX GDPR**:

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

The screenshot shows a window titled "New Processed Personal Data". It contains the following sections:

- Data Categories:** Includes buttons for "Contact" and "Cookies and System Logs".
- Data Subjects Categories:** Includes buttons for "Agents", "Customers", and "Employees".
- Risk:** Shows a yellow warning icon and the text "Medium".
- Number of Records:** Shows a text input field with the value "10-1000".

In this window you can specify the following information:

- **Data categories**
- **Data subjects**
- **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 a important principle of the European Union's General Data Protection Regulation (GDPR).

According to article 5 of the GDPR, 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 repurposed 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 GDPR team can later give a compliance score for the Personal Data Risk section based on the information completed by the activity owner:

- 1 Select a value from the **Data Minimization 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 [Defining 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 [.](#)
- 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.


— Data Subjects' Rights & Notice Management of Full Processing


Specify in the following section which data subjects' rights are granted and, if relevant, attach any processing activity specific document in the attachment section (eg. a specific SOP for data subjects' request management which applies to this processing activity in particular).


 ☐ Access


 ☐ Objection

 ☐ Restriction

 ☐ To be forgotten

 ☐ Deletion

 ☐ Portability

 ☐ Rectification

**Notice:**

☐ Yes, written

☐ Yes, oral

☐ No


☐ Not required

☐ Don't know

**Consent:**

☐ Yes


☐ No

 Data Subjects' Rights & Notice Management Compliance Level:


▼

## 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 GDPR** provides a report for this.

To have a general view of the data subject rights:

- 1 In the activity owner desktop, click **Reports > Data Subjects' rights**.

## Giving a compliance score for data subject rights

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

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

---

## Data Transfers



*Under the GDPR, 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 [Defining 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 GDPR 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 GDPR 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 GDPR 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 Agreements** tab.
3. Click **New**.
4. Fill in the fields as appropriate:
  - **Contract name**
  - **Contract scope**
  - **Expiration date**
  - **GDPR 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:

The screenshot shows the 'Payroll Management' interface. At the top, there's a header with 'Payroll Management' and a status indicator 'Status: \* Live'. Below the header, there are tabs: 'Overview', 'Legal Basis', 'Details' (selected), 'Preassessment', and 'DPIA'. Under the 'Details' tab, there's a sub-tab 'Details View' and 'Assessment View'. A table is displayed with columns: 'Processing Element', 'Type', 'Organization', and 'Data Protection Role'. The first row in the table is highlighted and labeled 'Processing activity' and 'Processing element' with blue arrows. The row contains the text 'GDPR Application Processing', 'Third Party', 'HQ Entity', and 'Data Controller'.

## 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 GDPR**, select one of them in the corresponding drop-down list.

The screenshot shows the 'New Element' form. It has a title bar 'New Element' with a plus icon and a refresh icon. The form contains several fields: 'Type \*' with a dropdown menu showing 'Application'; 'Application \*' with a dropdown menu showing 'ERP'; 'Organization \*' with a dropdown menu showing 'XCorp HQ'; 'Data Protection Role \*' with a dropdown menu showing 'Data Processor'; 'Element Name' with a text input field; and 'ID' with a text input field.

4. Click **OK**.

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

Processing Element ↑	Type
Payroll Management	
Payroll Management	Application

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.

New

Processing Element ↑	Type
HR Management	
HR Management System	Application

Open web site involving the application

Application properties

## USING THE PROCESSING ACTIVITY WORKFLOW

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

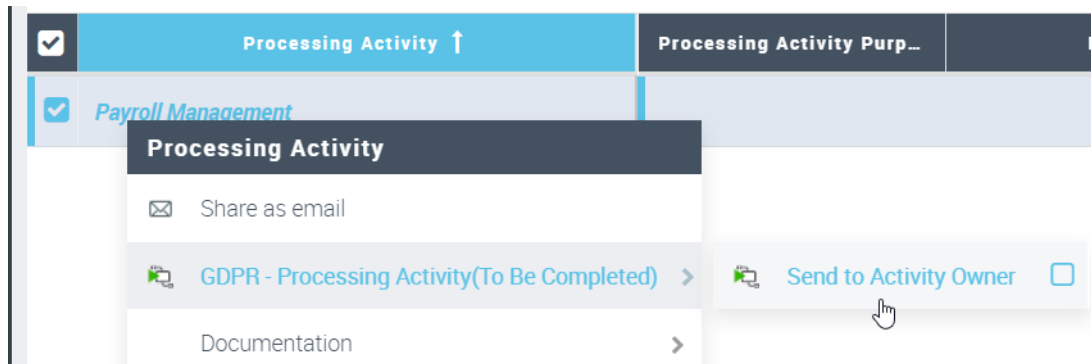
The chief privacy officer creates the processing activity. He asks the activity owner to complete the processing activity description. Once the processing activity has been described, the chief privacy officer can validate it. Then, pre-assessment and eventually DPIAs can be performed.

➤ For more information on the complete workflow, see [What are the possibilities offered by the standard processing activity workflow?](#)

### Asking the activity owner to complete processing activity description

To send the processing activity to the activity owner:

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



The activity owner can then connect to **HOPEX GDPR** with the corresponding profile and complete the description of the processing activity.

➤ You must have previously selected an activity owner in the processing activity property page.

## Submitting processing activity description

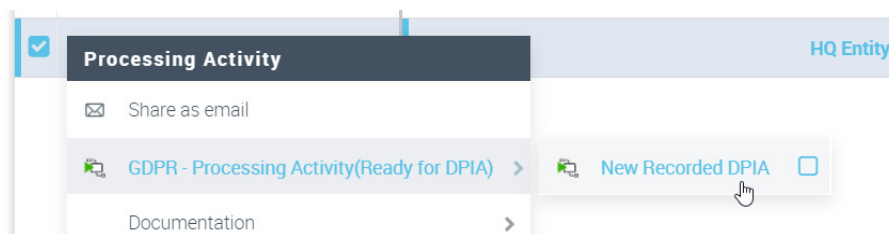
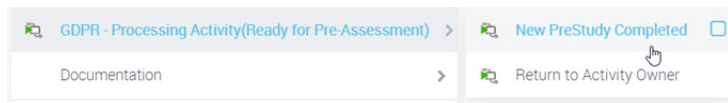
After completing the processing activity description, the activity owner can send it to the GDPR team, who will in be able to start a pre-assessment based on what the activity owner specified.



## Submitting pre-assessments and DPIAs

After the activity owner 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 GDPR team might want to return it to the activity owner for review.*

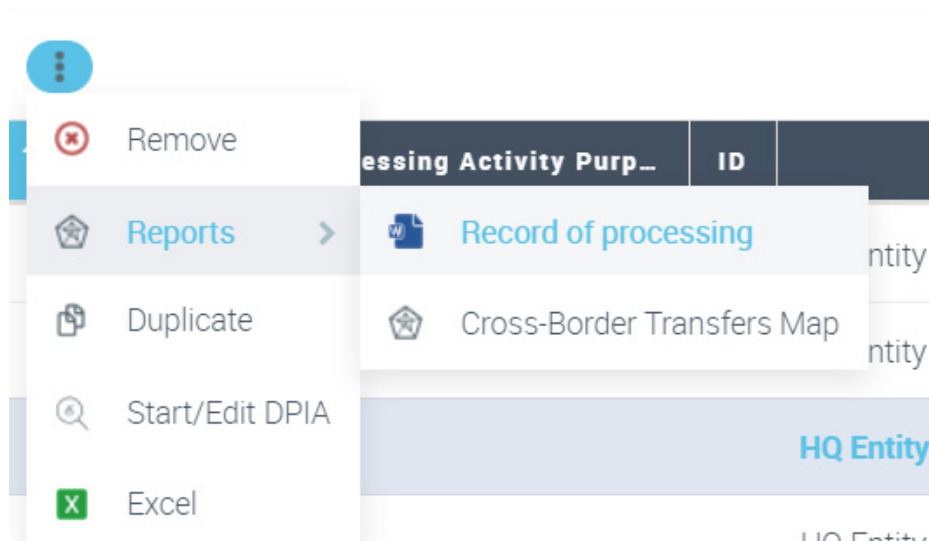


# PROCESSING-RELATED REPORTS

## 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 GDPR 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. In the navigation menu, click **Record of Processing**.
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

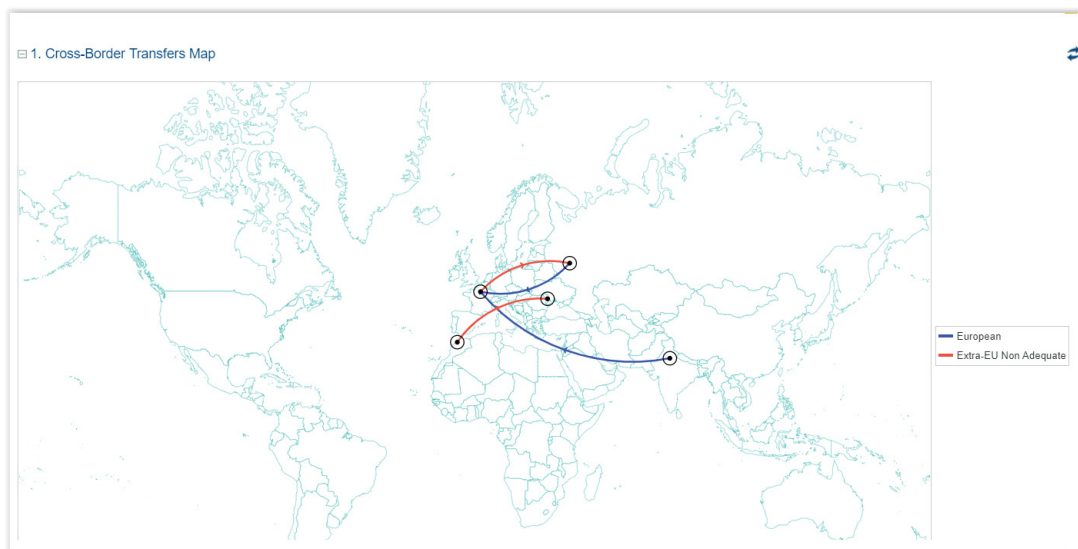
Make sure that:

- 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 GDPR** 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 **GDPR** 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 controller" in their property page.

### Generating the CNIL report

To generate this report:

1. In the navigation menu, select **Record of Processing**.
2. Select the processing activities of interest to you (those for which the "Data Controller" 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**.

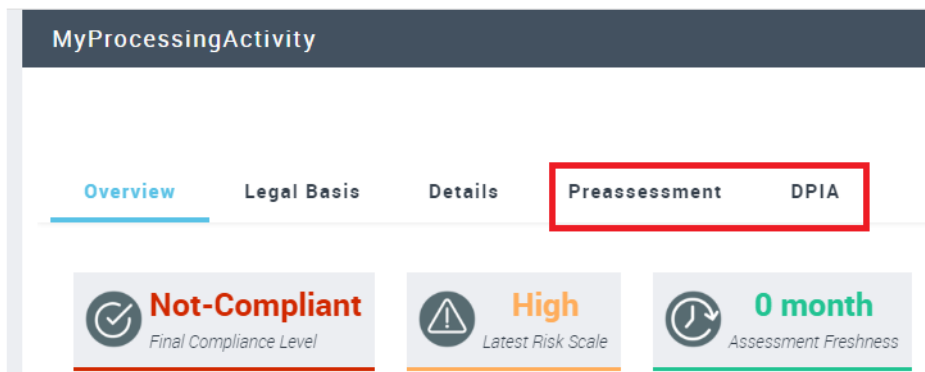
The Excel report is generated.

# ASSESSING PROCESSING ACTIVITIES

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

For more details on processing activities description, see [Describing Processing Activities in HOPEX GDPR](#).

As a GDPR team member assessing processing activities, you need to use the following tabs:



For assessment troubleshooting, see [About Assessments](#).

- ✓ [Prerequisites to Processing Activity Assessment](#)
- ✓ [Performing a Pre-assessment](#)
- ✓ [Performing Impact Assessment \(DPIA\)](#)

# PREREQUISITES TO PROCESSING ACTIVITY ASSESSMENT

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

- activity owners have properly described the processing activities  
☛ For more information, see [Describing Processing Activities in HOPEX GDPR](#).
- you have specified compliance levels on the basis of the information given by activity owners.  
☛ See [Specifying Compliance Levels](#).

---

## Specifying Compliance Levels

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

☛ It is necessary to give those scores after the activity owner 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** tab.
3. Select a value in the drop-down menu available

Overview Legal Basis Details Preassessment DPIA

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.

☒ Contractual Necessity ☐ Law Enforcement

☒ Vital Interest ☐ Legitimate Interest

☐ Public Interest ☐ Specific Consent

Description:



Legal Basis Compliance Level: Almost Compliant

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 property page.  
 See [Accessing Processing Activities](#).
2. Select the **Details** tab.
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 property page.  
 See [Accessing Processing Activities](#).
2. Select the **Details** tab.
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 GDPR 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-assessment or a DPIA).

To identify the compliance level of a processing activity:

1. In the processing activity property page, select the **Pre-assessment** tab.

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

**Payroll Management** Status: \* ● Live

Overview Legal Basis Details **Preassessment** DPIA

**i** Carry out a high level assessment of the processing activity based on the information provided in the previous sections. The scope of the pre-assessment is to identify those processing activities which require a DPIA (those characterized by a high risk) or require adjustments, having a low compliance level.

<b>Almost Compliant</b> Legal Basis	<b>Poorly Compliant</b> Data Minimization	<b>Compliant</b> Data Subjects' Rights & Notice Management
<b>Compliant</b> Data Transfers Compliance Level	<b>None</b> Security Measures Compliance Level	

- Legal Basis (score from the Legal Basis tab)
  - See [Processing Activities Legal Basis](#)
- Data Minimization (score from the Details tab)
  - See [Processed Personal Data](#)
- Data Subject's Rights & Notice Management (score from the Details tab)
  - See [Data Subject Right and Notice Management](#)
- Data Transfers (score from the Details tab)
  - See [Data Transfers](#)
- Security Measures (score from the Details tab)
  - 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 assigned by the activity owner for the processing activity. See [Viewing the Initial Compliance Level of a Processing Activity](#)

---

### Consulting Decision-Making Reports

In **HOPEX GDPR** you may use your dashboard to identify compliance priorities and perform an initial assessment. It will enable you to focus on the activities at risk whose compliance needs to be improved.

Your dashboard is pre-populated with 3 different charts in the form of a pie chart. They give an indication of:

- the final compliance level and risk scale after assessment of the processing activity.  
☛ See [Processing activities by compliance level](#) and [Processing activities by risk scale](#).
- which processing activities have already been assessed through a DPIA  
☛ See [Processing activities by assessment status \(DPIA\)](#)  
☛ Note that when you select a sector of the pie-chart, the corresponding processing activities are displayed at the bottom.

### Accessing your dashboard

To access your dashboard:

- 1 From the navigation menu, click **Dashboard**.

☛ The reports of your dashboard take into account all the objects you are allowed to view.

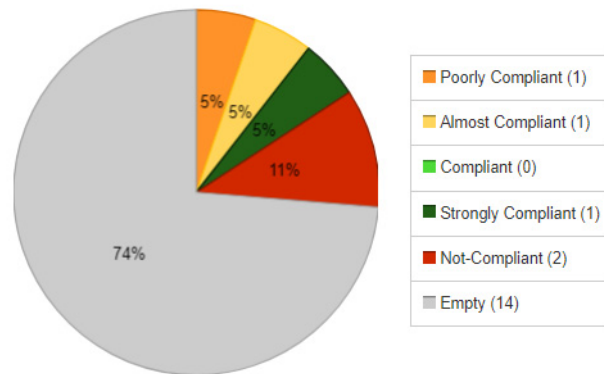
### Processing activities by compliance level

This pie chart enables you to view which processing activities are compliant.

☛ The information displayed is obtained through pre-assessments or DPIAs (the result of the most recent of the two is taken into account).

GDPR - Processing Activities by Compliance Level

Compliance Level

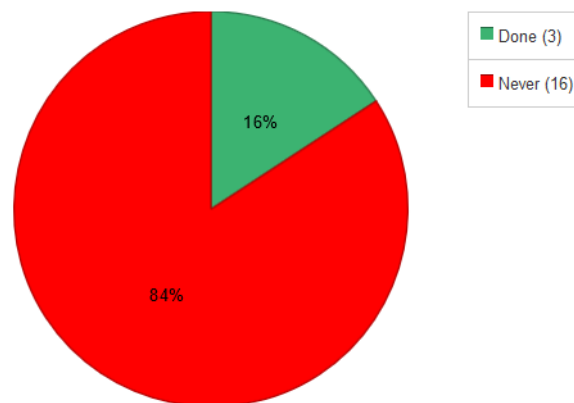


### Processing activities by assessment status (DPIA)

This pie chart illustrates the number of processing activities which have been assessed ***through a DPIA***. Those which have not been assessed through a DPIA require your attention.

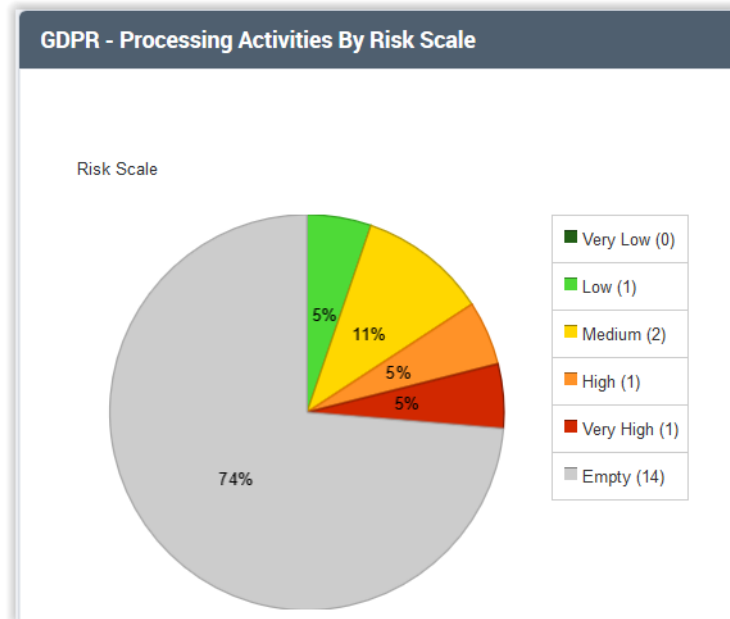
GDPR - Processing Activities By Assessment Status

Assessment Status



## Processing activities by risk scale

This pie chart shows which processing activities are considered at risk.



*The information displayed is obtained through pre-assessments or DPIAs (the result of the most recent of the two is taken into account).*

---

## 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** tab of the processing activity property page, unfold 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**.

Validation

Final Compliance Level \*

Compliant

Comment

Final Risk Level \*

Low

Comment

Subsequent Actions \*

Nothing

Comment

Preassessment Name \*

MyProcessingActivity-Preassessment

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:

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

Pre-assessments History			
Local name ↑	Completion Date	Final Compliance Level	Subsequent Actions
MyProcessingActivity-Preassessment	1/29/2019	Compliant	Nothing

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 GDPR 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 [Assessing Risks](#).

- the remediation actions ensuring the processing activity is under control

☛ For more information, see [Defining Recommendations and Remediation Actions](#).

---

## Creating a DPIA

### Starting a DPIA from scratch

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 [Assessing 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 exist 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 DPIA from scratch](#).*

---

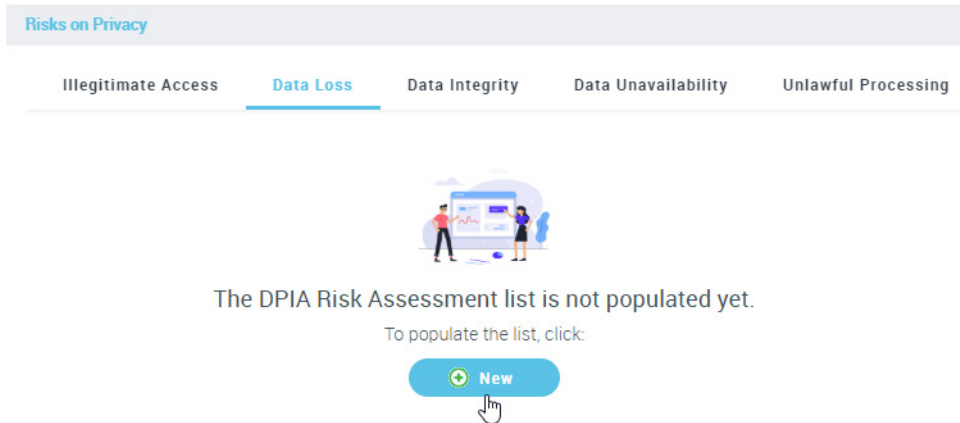
## Assessing Risks

The first step in DPIA creation consists in defining and assessing risks.

To assess risks in **HOPEX GDPR**:

1. In the property page of a processing activity, select the **DPIA** tab.
2. Click **Start DPIA**.
3. In the DPIA creation wizard, select one of the tabs of the **Risks on Privacy** section:
  - **Illegitimate Access**
  - **Data Loss**
  - **Data Integrity**
  - **Data Unavailability**
  - **Unlawful Processing**Here you can create a risk assessment corresponding to different risk types.

- Click **New**.



- Specify risk properties as shown below.

The screenshot shows a 'New Risk Assessment' form. The form has a dark header bar with the title 'New Risk Assessment' and two icons (a plus sign and a refresh/cancel icon). The form contains the following fields:

- Risk Name \***: A text input field containing 'DPIA Risk Assessment-1'.
- Risk Description**: A rich text editor with a toolbar showing icons for link, font color, bold, italic, underline, text color, and a menu icon. The text area is empty.
- Risk Severity \***: A dropdown menu with 'Low' selected (indicated by a green triangle icon).
- Likelihood \***: A dropdown menu with 'Likely' selected (indicated by a yellow triangle icon).
- Risk Cause**: A text input field.
- Data Subject Impact**: A text input field.
- Security Measures**: A text input field with a downward arrow icon at the bottom right.


- Enter the **Risk Severity** and **Risk Likelihood** for the risk you intend to assess.

👉 These fields are mandatory.

In addition, you can specify:

- **Data Subject Impacts:** main impacts on data subjects if the risk occurs
- **Risk cause:** most common causes which could lead to risk occurrence
- a group of **Security Measures** aimed at remediating the risk

**Prerequisites:** Security measures must have first been defined in the processing activity properties. See [Specifying security measures on a processing activity](#).


 *Security measures are reference data defined by the functional administrator. They can be of three types (technical, organizational, certification). For more information, see [Définir les mesures de sécurité](#).*

---

## Defining Recommendations and Remediation Actions

The second step when performing a DPIA is to define recommendations and remediation actions.

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

 *For more information, see [Assessing Risks](#).*

To create recommendations within the framework of a DPIA:

1. In the DPIA window, expand the **Recommendations and Remediation actions** section.

 *To access the DPIA window, see [Creating a DPIA](#).*

2. In the **Risk Description** field, select one or several risk assessments to connect to the recommendation being created.

You can also provide the following information for your recommendation:

- **Recommendation description:** give a comment for your recommendation
- **Resulting risk:** specify the intended risk obtained after the remediation actions have been implemented.

---

## Attaching Documents to the DPIA

You can attach documents (business documents) to the DPIA.

To do so:

- In the DPIA window, expand the **DPIA Attachments** section.

---

## Validating the DPIA

In this section the DPO needs to draw the conclusions of the DPIA:

### 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 Action

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

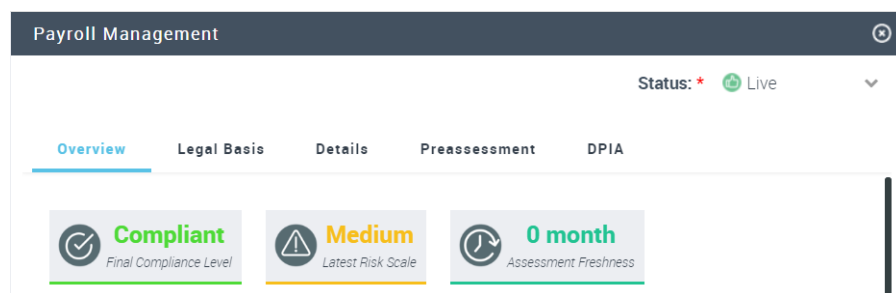
- Nothing
- Stop processing activity
- Notify supervisory authority

---

## 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.



### ***Final compliance level and Latest risk scales***

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

🔑 The most recent of the two is taken into account.

## Assessment freshness

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

## Record of DPIAs

See [Record of DPIAs](#)

## Generating a DPIA document

To generate a DPIA document:

1. In the **DPIA** tab of the processing activity property page, expand the **DPIA history** tab.
2. Select a DPIA and click **DPIA document**.

Local name ↑	Completion Date	Compliance Level	Subsequent Actions	Final Risk Level
DPIA on ProcessingA...	7/23/2018	Almost Compliant	Stop Processing Acti...	Very Low

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 GDPR** enables the data controller to keep a record of data breaches, as required by the law.

**HOPEX GDPR** 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 GDPR**.

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

To enter a data breach:

1. from the navigation menu, select **Personal Data Breach** and click **New**.

**New Data Breach**

**Status \***  
Submitted

**Data breach \***  
GDPR Data Breach-1

**Nature of breach**

**Number of impacted people**

**Involved Data Categories**

**Impacted Data Subjects**

**Date of Breach** **Date of discovery**

**Whistle-Blower** **Source**

OK Cancel

2. Describe the data breach as follows:

- **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
- **Date of breach**
- **Number of impacted people**
- **Source**: external claim, internal control, internal alert, other
- **Involved data categories**

☛ For more information, see [Defining Data categories](#).

- **Impacted data subjects**

☛ For more information, see [Defining Data Subject Categories](#).

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.

Data processed by subcontractor without proper authorization of the controller

Status: \* Submitted ▼

Overview   Breach Scope   Breach Assessment   Breach Notification

 Describe the scope of the data breach, i.e. which legal entities, departments and processing activities affected by the breach. The scope of the data breach also determines who can view the breach info.

Select all legal entities which are impacted by the breach

Select all departments which are impacted by the breach

Select all processing activities which are impacted by the breach

## Assessing a Data Breach

To assess a data breach:

1. In the navigation menu, click **Personal Data Breach**.
2. Select a data breach and in its property page, select the **Breach Assessment** tab.

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 menu, click **Data Breach Management**.
2. Select a data breach and in its property page, select the **Breach Assessment** tab.
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:
  - Implemented
  - Ongoing
  - Foreseen

 *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 menu, click **Personal Data Breach**.
2. Select a data breach and in its property page, select the **Breach Notification** tab.

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**
  - **GDPR authorities notification date**

---

## Viewing Elapsed Time since Breach Discovery

You have 72 hours to take action on detection of the breach and notify authorities or data subjects.

**HOPEX GDPR** automatically computes this piece of information for you.

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

1. In the navigation menu, click **Personal Data Breach**.
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:

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

1. In the navigation menu, click **Personal Data Breach**.
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



The GDPR gives 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 GDPR** 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 menu, click **Data Subject Management > Data Subject Requests**.
2. Click **New**.



You can 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:

- **Request source**  
The request source is the means through which the request is received.  
*Example: the ID of a web form*
- **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
- **Data Subject Request**  
 A comment can be entered here.
- **Request Priority**
  - High
  - Medium
  - Low
- **Assigned person**
- **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 menu select **Data Subject Management > Data Subject Request**.
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 menu select **Data Subject Management > Data Subject Request**.
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 menu select **Data Subject Management > Data Subject Request**.
2. In the columns available on the data subject request, select the **Deadline extended** check box.

# DEMONSTRATING COMPLIANCE



**HOPEX GDPR** enables you to create reports showing the compliance and accountability level of processing activities.

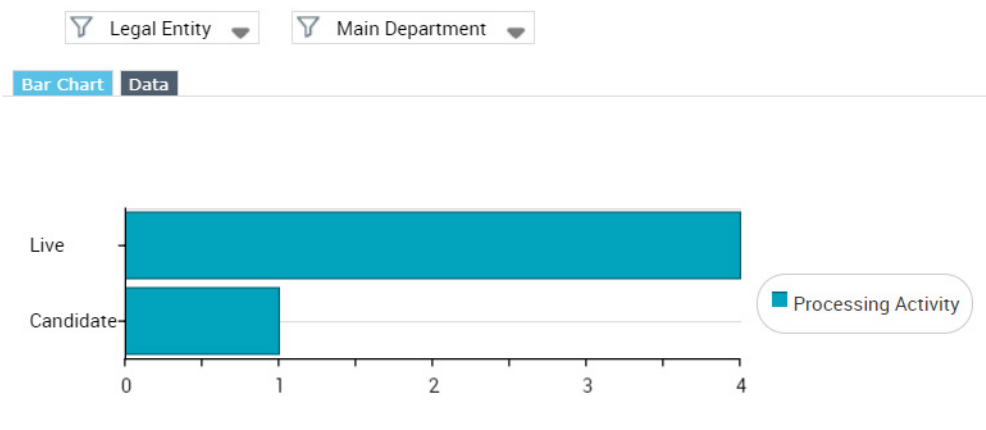
To access reports:

- 1 From the navigation menu, 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

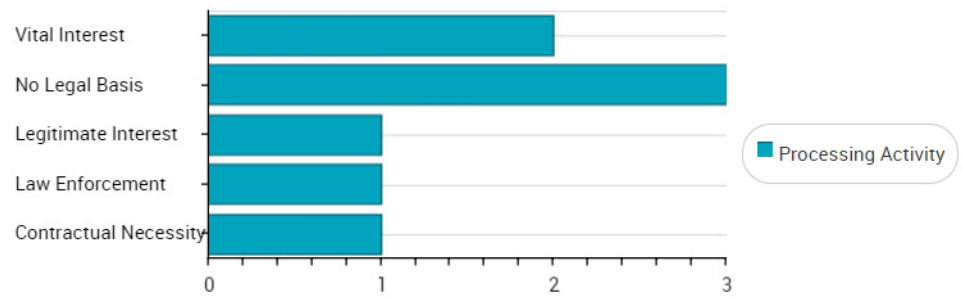
This report displays the processing activities grouped by legal basis. It also helps identify those which don't have one yet.

Department ▼

Legal Entity ▼





















Bar Chart

Data



## Sensitive Activities

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

Sensitive Activity 	
Sensitive Activity	Processing Activity
 Automated decision making with legal or similar significant effect	
 Automated processing of sensitive data	
 Evaluation or scoring, including profiling and predicting	
 Innovative use or application of new technological or organizational solutions	 Processing Activity-1
	 Processing Activity-2
 Large scale systematic monitoring of publicly accessible areas	 Processing Activity-1
	 Processing Activity-plt
 Large-scale processing operations of sensitive data	
 Matching or combining data sets	
 Processing of data concerning vulnerable data subjects	
 Processing of data on a large scale	
 Processing of sensitive data or data of a highly personal nature	 Payroll Management
 Processing preventing data subjects' rights exercise	 Payroll Management
 Profiling	
 Systematic monitoring	

## Record of DPIAs

To launch this report:

- 1 In the navigation menu select **Reports > Standard Reports > Record of DPIAs**.

This report displays the different DPIAs which have been performed on the processing activities you can access. The following information is displayed:

- assessment name
- processing name
- DPO
- department
- compliance level
- final risk level
- completion date

To generate a DPIA document for a particular DPIA:

- 1 Select a DPIA and click **DPIA Document**.

For more information on DPIAs, see [Performing Impact Assessment \(DPIA\)](#).

## Data Risk Report

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

To launch the data risk report:

- 1 In the navigation menu select **Reports > Standard Reports > Data Risk Report**.

This report contains two tables:


- one for data categories
  - For more information, see [Defining Data categories](#).
- the other for data subjects categories.
  - For more information, see [Defining Data Subject Categories](#).

Data Category	Default Data Risk Level	Processing Activity	Pre Assessment	Risk Level	Compliance Level	DPIA	Final Risk Level	Final Compliance Level
Biometric	High		No			No		
Cookies and System Logs	Medium	ProcessingActivity-2	Yes (7/23/2018)	Medium	Poorly Compliant	Yes (7/23/2018)	Very Low	Almost Compliant
Education			No			No		
Financial	High	ProcessingActivity-1	Yes (7/23/2018)	High	Almost Compliant	No		
Health	High	ProcessingActivity-2	Yes (7/23/2018)	Medium	Poorly Compliant	Yes (7/23/2018)	Very Low	Almost Compliant
		ProcessingActivity-1	Yes (7/23/2018)	High	Almost Compliant	No		


Data subject category	Default Data Risk Level	Processing Activity	Pre Assessment	Risk Level	Compliance Level	DPIA	Final Risk Level	Final Compliance Level
Clients	Medium	ProcessingActivity-1	Yes (7/23/2018)	High	Almost Compliant	No		
Customers			No			No		
Drivers	Medium	ProcessingActivity-2	Yes (7/23/2018)	Medium	Poorly Compliant	Yes (7/23/2018)	Very Low	Almost Compliant
Internet customers		ProcessingActivity-2	Yes (7/23/2018)	Medium	Poorly Compliant	Yes (7/23/2018)	Very Low	Almost Compliant
Loan applicant (25 - 45 yo)			No			No		
			No			No		

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 Transfers

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](#).






















## Data Subject Rights Report


To display the Data Subject Rights report:

- 1 In the navigation menu select **Reports > Standard Reports > Data Subject Rights Report**.

This report contains all processing activities with the rights of data subjects which have been considered.

### 1. GDPR - Right compliance

	Access	Deletion	Objection	Portability	Rectification	Restriction	To be forgotten
Accounting							
Legal							
Purchasing							

 For more information on data subject rights, see [Data Subject Right and Notice Management](#).


## Third-Parties Report

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.

Payroll Management				
Status: *  Live				
Overview	Legal Basis	Details	Preassessment	DPIA
Processing Element ↑	Type	Organization	Data Protection Ro...	
Payroll Management				
Payroll subcontractor	Third Party	HQ Entity	Data Processor	

## Launching the Third-party report







To display the third-party report:

- › In the navigation menu select **Reports > Standard Reports > Third Parties Report**.

## Third-party report content

It gives the following information for each third-party:

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

1. Active Third-Parties				
Third-Party Name	Processing Activity	Raw Risk	Compliance Level	Last Assessment Date
Africa lear	Accidents and diseases	 Medium	 Almost Compliant	7/2/2018
2. Obsolete Third-Parties				
Third-Party Name	Processing Activity	Raw Risk	Compliance Level	Last Assessment Date
casa bear shore	Email Marketing	 High	 Poorly Compliant	6/26/2018
	Employee training Management	 Very Low	 Compliant	7/2/2018

The report distinguishes between:

- active third-parties
- obsolete third-parties


## Record of Processing

**HOPEX GDPR** enables you to automatically generate the record of processing.

See [Processing-Related Reports](#) for a description of reports available on processing activities.

## Cross-border transfer map



To generate the cross-border transfer map:











- 1 Select the transfers of interest to you and click 

See [Cross-border transfer map](#) for a description of this report.

## IT Applications

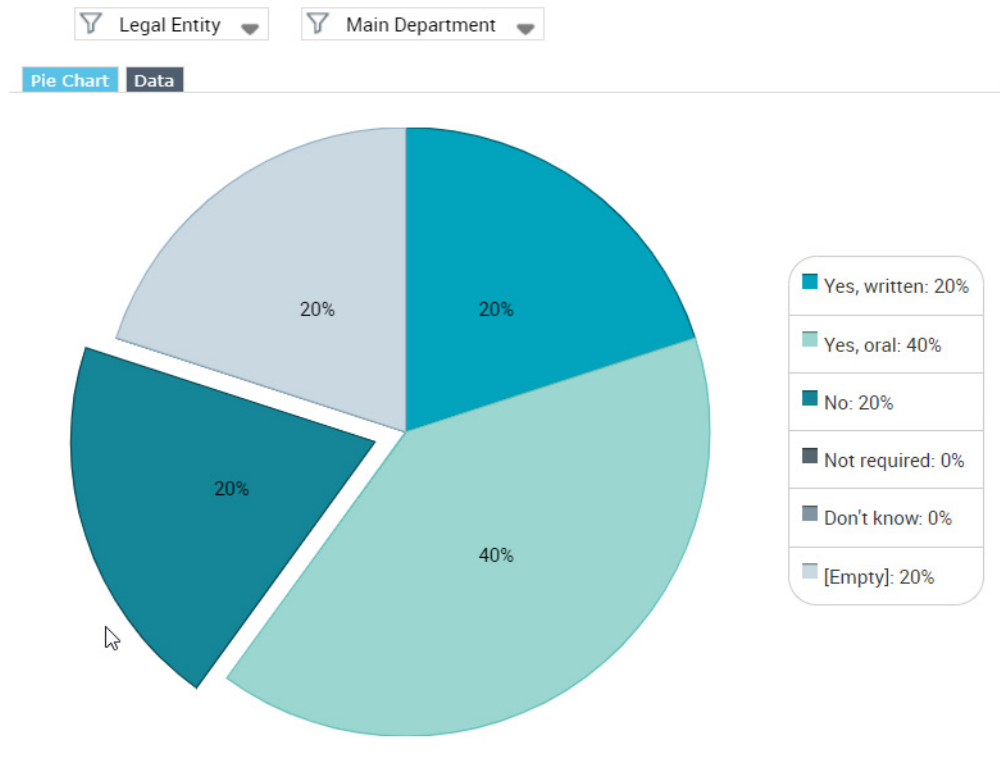
This report contains a list of all IT applications involved in the existing processing activities.

 Processing Activity 

Processing Activity	GDPR Application	Application Name
 Processing Activity-1		
 Processing Activity-1		
 Cancel Package	 Accounting	Accounting
	 Asset Management	Asset Management
 Payroll Management	 Payroll Application	
	 Payroll Application	
 Processing Activity-plt	 Asset Management	Asset Management

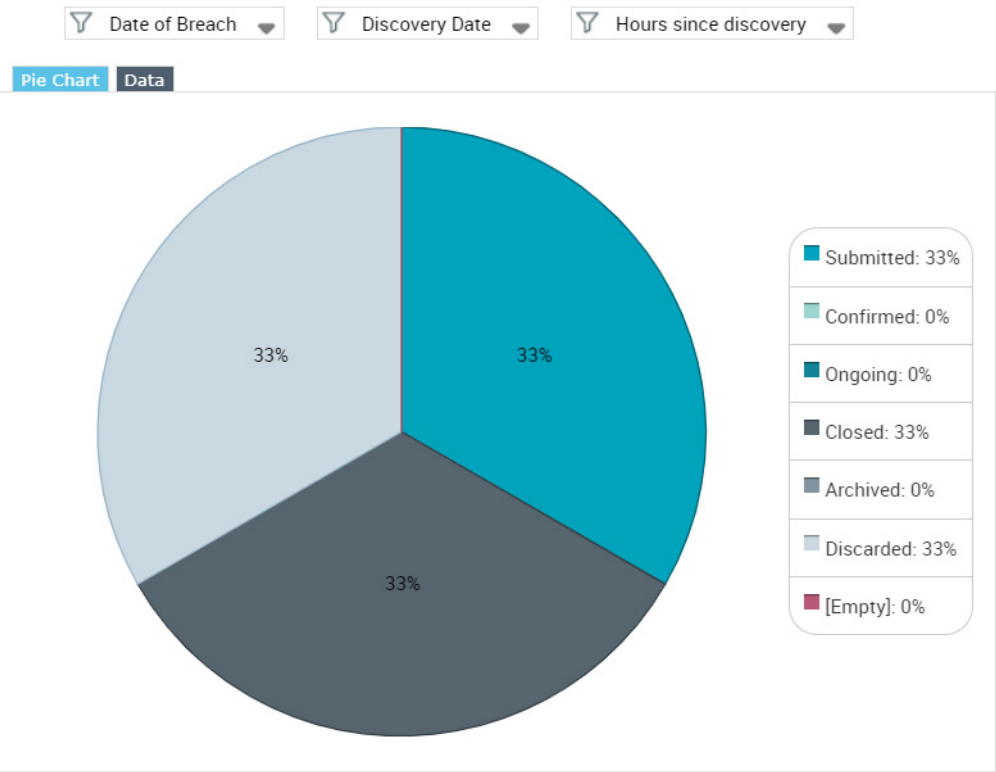
## Notice

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



## Data Breaches

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





# FAQs



---

## About Processing Activities

🔖 For general information on processing activities, see [Describing Processing Activities in HOPEX GDPR](#).

### 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](#).

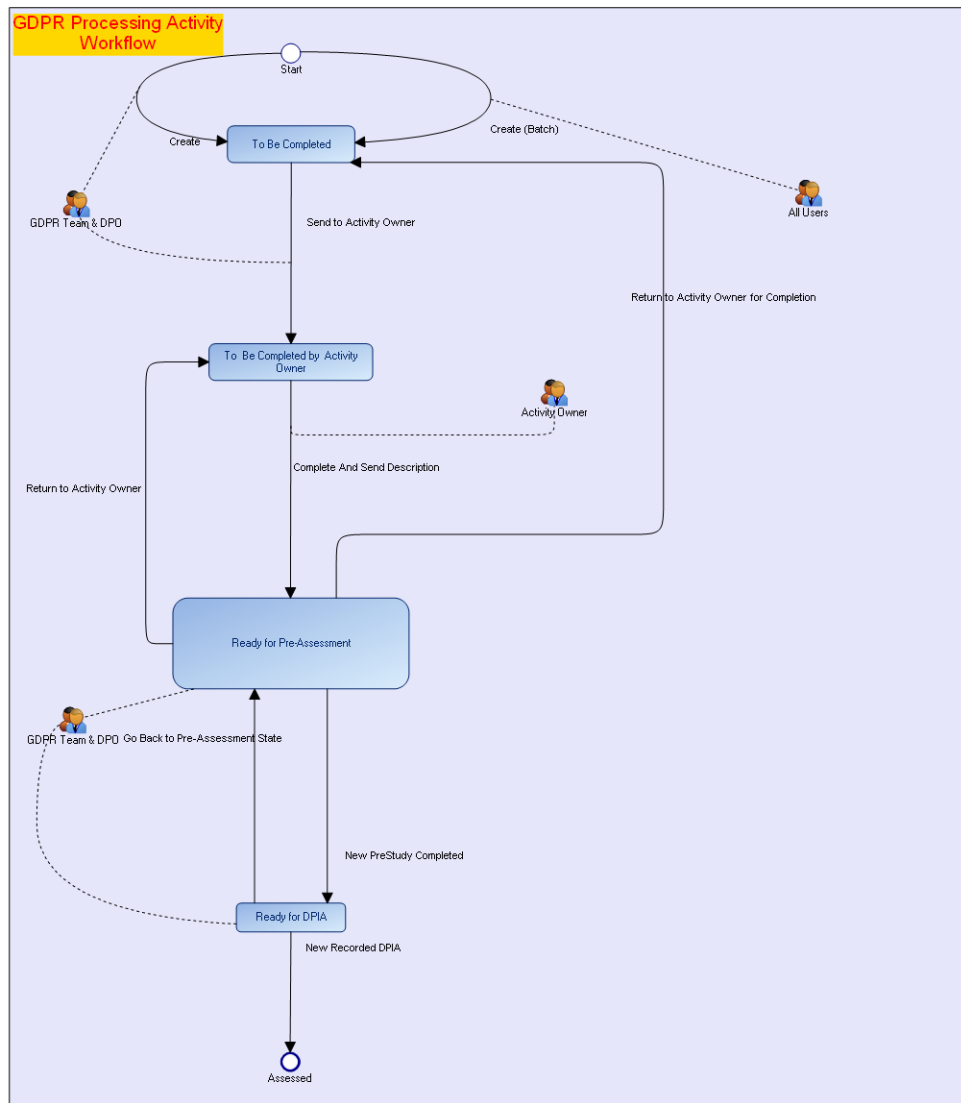
### How can I produce a Word version of my record of processing?

See [Creating a record of processing](#).

### An application is involved in one of my processing activity. I need to describe specifically how this part of the processing activity is handled. What should I do?

**HOPEX GDPR** 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 [Consulting Decision-Making Reports](#)
    - ☞ *This information concerns the processing activities which have already been assessed.*
- the **final risk level** of your processing activities
  - ☞ See [Consulting Decision-Making Reports](#)
- the **assessment status** (DPIA)
  - ☞ See [Consulting Decision-Making Reports](#).

## 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 GDPR**:

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 [Record of DPIAs](#).*
- From the **DPIA** tab of the processing activity property page.
  - ☞ *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](#).*

---

## 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 GDPR** 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 GDPR Import and HOPEX Integration

### How can I reuse information from other HOPEX solutions?

**HOPEX GDPR** enables you to:

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

☛ *For more information, see [Creating Processing Activities from HOPEX Objects](#).*

- view application/process properties and associated diagrams directly from **HOPEX GDPR**.

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

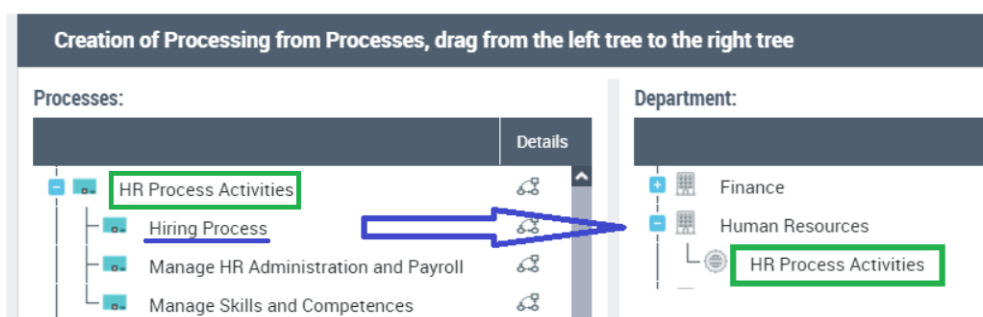
It is possible to drag-and-drop sub-processes to create a processing activity but there is a specific rule for it:

***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. From the navigation menu click **Record of processing**.
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 GDPR**.

### 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 GDPR functional administrator can create legal entities or departments.

Make sure you are connected with the appropriate profile.



## GDPR GLOSSARY

<b>Activity Owner</b>	The activity owner provides a detailed description of the processing activity (excluding assessment).
<b>Binding Corporate Rules (BCRs)</b>	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).
<b>Computing Device</b>	Computing devices are hardware pieces that can host and run software. Together with their hosted applications, they provide Information and IS services.
<b>Company Guideline</b>	Company guidelines enable you to attach documents or specify a URL concerning GDPR-relevant information the organization might use to give evidence of the company accountability .
<b>Consent</b>	Consent is a freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.
<b>Data Category</b>	Data category is used to group different personal data.
<b>Data Controller</b>	A data controller is the entity that determines the purposes, conditions and means of the processing of personal data.
<b>Data Erasure</b>	See Right to be forgotten.
<b>Data Portability</b>	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.
<b>Data Processor</b>	A Data Processor is the entity that processes data on behalf of the Data Controller.
<b>Data Protection Authority</b>	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.

<b>Data Protection Officer</b>	The Data Protection Officer (DPO) works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.
<b>Data Subject</b>	A Data Subject is a natural person whose personal data is processed by a controller or processor.
<b>Data Transfer</b>	Under the GDPR, a data transfer is a transfer or copy of personal data.
<b>DPIA</b>	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 the GDPR, data protection impact assessments are mandatory in certain cases such as profiling.
<b>Data Subject Category</b>	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.
<b>Data Subject Request</b>	A data subject request is a formal request by a data subject to a controller to take action on his/her personal data.
<b>Deputy DPO</b>	A deputy DPO may assist the DPO in large organizations.
<b>Establishment</b>	An establishment corresponds to the location (site) of a legal entity.
<b>Joint Controller</b>	Joint controllers can work jointly to determine the purposes and means of a processing activity.
<b>IT Support Correspondent</b>	An IT support correspondent is in charge of providing IT support.
<b>Risk</b>	A risk represents any risk related to data privacy that should be identified and assessed during a DPIA process.
<b>Legal Entity</b>	A Legal Entity is a company or an organization which has legal rights and obligations.
<b>Minimization</b>	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.
<b>National Representative</b>	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.

<b>Organizational Chart</b>	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.
<b>Personal Data</b>	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.
<b>Personal Data Breach</b>	Personal Data Breach is a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data.
<b>Physical Archive</b>	A physical archive corresponds to the premises in which historical records are located.
<b>Privacy by Design</b>	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.
<b>Processing Activity</b>	A processing activity consists of any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.
<b>Profiling</b>	Profiling consists of any automated processing of personal data intended to evaluate, analyze, or predict data subject behavior.
<b>Purpose</b>	The purpose of a processing activity is the main objective of this processing activity. Examples: satisfaction survey, customer management, site monitoring.
<b>Record of Processing Activities</b>	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.
<b>Representative</b>	A representative is a person in the European Union explicitly designated by the controller to be addressed by the supervisory authorities.
<b>Retention Period</b>	A retention enables to record the time lapse in which the data personal will be stored by the organization.
<b>Right to Access</b>	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.

**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.