HOPEX Privacy Management

Guide d’utilisation

HOPEX Aquila

MEGA
SEE THE BIGGER PICTURE

SOMMAIRE

Sommaire

Sommaire

INTRODUCTION À HOPEX PRIVACY MANAGEMENT

HOPEX Privacy Management est une solution qui vous permet de gérer la conformité à des lois de protection de données personnelles telles que RGPD.

La solution fournit un espace de travail collaboratif aux DPO ainsi qu'aux différentes parties prenantes.

Elle vous permet de produire les documents qui attestent que vous maîtrisez la confidentialité des données à caractère personnel et que vous avez adopté les mesures de sécurité qui conviennent.

HOPEX Privacy Management intègre les informations réglementaires et des modèles juridiques mis à jour régulièrement pour accélérer votre mise en conformité.

HOPEX Privacy Management vous permet de réutiliser les acteurs, processus et applications créés dans **HOPEX Business Process Analysis**, **HOPEX IT Architecture** et **HOPEX IT Portfolio Management**.

- ✓ Conditions préalables à HOPEX Privacy Management
- ✓ Se connecter à HOPEX Privacy Management
- ✓ Profils utilisés dans HOPEX Privacy Management
- ✓ Fonctionnalités utiles

Conditions préalables à HOPEX Privacy Management

La première fois que vous installez **HOPEX Privacy Management**, vous devez importer le module Privacy Management Content (hopex.privacy).

Pour plus de détails, voir Importer un module dans HOPEX.

SE CONNECTER À HOPEX PRIVACY MANAGEMENT

Pour vous connecter à **HOPEX Privacy Management** :

1. Lancez l'application **HOPEX** à partir de son adresse HTTP.

   ☛ *Si vous ne connaissez pas cette adresse, veuillez contacter votre administrateur.*

   La page de connexion apparaît.
2. Dans le champ **Login**, saisissez votre identifiant.
3. Dans le champ **Password**, saisissez votre mot de passe.
4. Dans le menu déroulant des environnements, sélectionnez votre environnement.

   ☛ *Si vous n'avez accès qu'à un environnement, celui-ci est automatiquement pris en compte et le champ de sélection de l'environnement n'apparaît pas.*
5. Cliquez sur **Sign in**.
   Lorsque vous êtes authentifié, une nouvelle fenêtre apparaît.
6. Dans le menu déroulant des référentiels, sélectionnez votre référentiel de travail.

   ☛ *Si vous n'avez accès qu'à un référentiel, celui-ci est automatiquement pris en compte.*
7. Dans le menu déroulant des profils, sélectionnez le profil avec lequel vous voulez travailler.
   Pour plus d'informations sur les profils, voir Profils utilisés dans HOPEX Privacy Management.

   ☛ *Si vous n'avez accès qu'à un référentiel, celui-ci est automatiquement pris en compte.*
8. Cliquez sur **Privacy Policy** et lisez la politique de confidentialité, puis sélectionnez **I have read and accept the privacy policy**.
   Le bouton **LOGIN** est actif.

   ☛ *Une fois que vous avez lu et accepté les consignes de politique de confidentialité, un certificat est automatiquement lié à votre personne et cette étape ne vous est plus jamais demandé.*
9. Cliquez sur **LOGIN**.

   ☛ *Cliquez sur **Back** si vous voulez revenir à la fenêtre d'authentification.*

   La page d'accueil de votre bureau apparaît et une session est ouverte.

   ☛ *Après une certaine période d'inactivité, vous êtes déconnecté de votre bureau. Pour vous reconnecter, suivez les étapes de la procédure ci-dessus. Cette période d'inactivité est configurée par l'administrateur du portail.*

PROFILS UTILISÉS DANS HOPEX PRIVACY MANAGEMENT

Résumé des profils

Profils	Définition
Propriétaire de traitement	Le propriétaire de traitement est un opérationnel responsable de la description des traitements de son périmètre d'activité (données, personnes concernées, transfert, etc.) Il fournit une description détaillée du traitement.
Responsable de la protection des données (DPO)	Le DPO joue le rôle de conseiller dans l'entreprise, de correspondant en matière de conformité auprès de l'autorité de contrôle, et de point de contact concernant les demandes des personnes concernées. Le DPO (Data Protection Officer) ou Responsable de la protection des données travaille de manière indépendante pour s'assurer de la bonne application des textes juridiques concernant les lois de protection des données. Il possède les droits sur l'ensemble des objets concernés par la confidentialité des données. Il édite les traitements, lance les pré-évaluations ainsi que les DPIA.
Responsable de la confidentialité	Le responsable de la confidentialité dirige le programme de conformité de l'entreprise et est responsable de sa mise en œuvre. Il s'assure que les experts disposent de toutes les informations dont ils ont besoin. Il possède les droits sur l'ensemble des données de référence (par exemple : les catégories de données, les mesures de sécurité.) Il est chargé de définir l'environnement. Le responsable de la confidentialité (RGPD) affecte les priorités et évalue les risques des traitements avec le DPO. Il s'assure que les données collectées sont suffisantes pour répondre aux exigences de la réglementation.
Équipe Privacy	L'équipe Privacy est constituée d'opérationnels qui suivent les instructions du DPO ou du responsable de la confidentialité. Ce profil peut être utilisé par n'importe quel membre de l'équipe Privacy.

Droits par profil HOPEX Privacy Management

Le Responsable de la confidentialité peut tout voir (menus de l'application et objets du référentiel)

Actions	Propriétaire de traitement/Propriétaire d'application	Responsable de la confidentialité	DPO/ Équipe Privacy
Accéder à l'environnement de Privacy (Section **Éléments clés**) - Catégories de données - Catégories de personnes concernées - Activités sensibles - Sécurisation des transferts - Autorités de contrôle - Adéquation Pays - Mesures de sécurité		X	X
Définir l'organisation (Section **Organisation**) - Entités juridiques - Départements - Tiers - Organigramme des DPO - Directives de l'entreprise		X	
Gérer les traitements (Section **Traitements**)	X	X	X
Gérer les réglementations		X	X
Réaliser une évaluation préliminaire Section **Traitements** > onglet **Évaluation préliminaire** - Identifier le niveau de conformité - Identifier le niveau de risque		X	X

Actions	Propriétaire de traitement/Propriétaire d'application	Responsable de la confidentialité	DPO/ Équipe Privacy
Réaliser une analyse d'impact (DPIA) Section **Traitements** > onglet **DPIA** - Définir les risques - Définir les recommandations et les mesures correctives		X	X
Gérer les violations de données Section **Violations**		X	X
Gérer les demandes des personnes concernées Section **Personnes concernées**		X	X
Plans d'action Gérer les plans d'action- - Soumettre des plans d'action	X	X	X

FONCTIONNALITÉS UTILES

> ☛ *Pour plus de détails sur l'utilisation du bureau et du référentiel, voir Manipuler les objets du référentiel.*

Statut de l'objet

Les objets de l'environnement possèdent un statut dans **HOPEX Privacy Management**.

Les objets de votre environnement peuvent avoir pour statut :

- **Candidat** : à valider par le DPO / l'équipe Privacy
- **Opérationnel** : a été créé et validé par le DPO / l'équipe Privacy
- **Obsolète** : n'existe plus

Vous pouvez spécifier le statut d'un objet dans la partie supérieure droite de l'objet, par exemple un traitement.

Fonctionnalités collaboratives

HOPEX Privacy Management facilite le travail d'équipe et propose différents moyens de communication. Vous pouvez :

- Créer et participer à des notes de révision sur les objets
- Ajouter des tags

  > ☛ *Les tags peuvent être utilisés dans le cadre de la recherche rapide pour retrouver un objet particulier. Voir La recherche plein texte.*
- Visualiser vos activités
- Partager avec d'autres utilisateurs **HOPEX** : ajouter des balises, aimer un objet.

  > ☛ *Pour plus de détails, voir Communiquer dans HOPEX.*

Fonctionnalités de recherche

HOPEX Privacy Management vous permet d'effectuer des recherches sur le référentiel.

Pour plus de détails, voir Recherche.

RÉUTILISER LES DONNÉES D'ARCHITECTURE D'ENTREPRISE

HOPEX permet de réutiliser les données déjà créées dans d'autres solutions **HOPEX** pour construire votre environnement de travail Privacy.

Vous pouvez :

- ✓ transformer les acteurs AE en organisations
- ✓ réutiliser les processus et applications pour créer les traitements dont vous avez besoin.

TRANSFORMER DES ACTEURS EA D'HOPEX EN ORGANISATIONS

Dans **HOPEX IT Portfolio Management** et **HOPEX IT Architecture**, des acteurs sont utilisés pour décrire l'organisation globale. Pour réutiliser des objets d'**HOPEX**, il peut être nécessaire de transformer des acteurs en organisations afin qu'ils soient reconnus dans **HOPEX Privacy Management**.

Transformer des acteurs EA en organisations

Pour transformer des acteurs EA en organisations:

1. Dans le menu de navigation, cliquez sur **Intégration > Organisation**.
2. Sélectionnez les acteurs qui vous intéressent et cliquez sur **Transformer**.
3. Dans l'assistant qui apparaît, sélectionnez le type de transformation à appliquer:
   - **Transformer en entité juridique**

     📖 *Une entité juridique est une entreprise ou organisation qui a des droits et obligations juridiques.*
   - **Transformer en département**

     ☛ *Si vous sélectionnez « Département » vous devez sélectionner l'entité juridique à laquelle doit être relié le département.*
   - **Transformer en tierce partie**

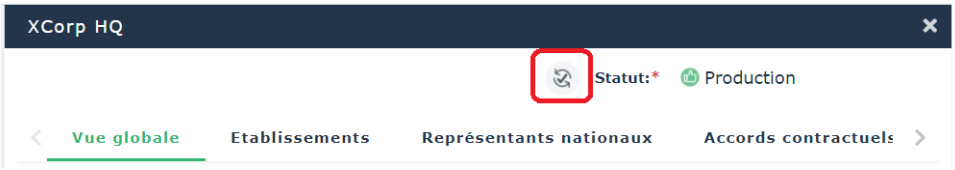
     📖 *Un tiers est une personne physique ou morale, une autorité publique, un service ou un organisme autre qu'une personne concernée, un responsable de traitement, un sous-traitant et les personnes qui, placées sous l'autorité directe du responsable de traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.*
4. Cliquez sur **OK**.

Vous pouvez voir les entités juridiques/départements/tierces parties créés à partir du menu **Organisation**.

☛ *D'un point de vue technique, la transformation crée un lien entre l'organisation et l'acteur AE (Architecture d'Entreprise). L'organisation hérite du nom local de l'acteur, qui devient l'entité juridique, la partie tierce ou le département.*

Synchroniser une organisation Privacy-AE

Lorsqu'un objet est modifié dans **HOPEX**, vous pouvez faire une synchronisation dans **HOPEX Privacy Management**. Dans la page de propriétés de l'organisation qui correspond à l'acteur modifié, le bouton **Synchroniser** est affiché.



Pour activer l'option de synchronisation :

1. Dans le menu principal, sélectionnez **Paramètres > Options**.
2. Dans la section **Privacy Management**, cochez « Afficher les boutons de synchronisation pour l'intégration Privacy-AE ».

CRÉER DES TRAITEMENTS À PARTIR D'OBJETS HOPEX

HOPEX Privacy Management vous permet de réutiliser des processus et des applications d'autres solutions.

☛ *Vous pouvez également créer des traitements directement dans HOPEX Privacy Management. Voir Créer les traitements.*

Créer des traitements à partir de processus

Vous pouvez utiliser des processus métier ou organisationnels disponibles dans d'autres solutions **HOPEX** pour créer des traitements.

Pour créer un traitement à partir d'un processus :

1. Dans le menu de navigation, cliquez sur **Intégration > Processus**. Un assistant apparaît.
2. Sélectionnez un processus dans l'arbre de gauche et glissez-le dans l'arbre de droite ***sous un département spécifique***.

Un traitement est créé. Vous pouvez maintenant y accéder à partir du registre de traitements. Pour plus de détails, voir Accéder aux registre des traitements.

☛ *Si vous rencontrez des difficultés dans la création d'un traitement à partir d'un sous-processus, veuillez vous référer à la section Questions fréquentes. Voir A propos de l'import et de l'intégration avec HOPEX.*

Créer des éléments de traitement à partir d'applications

Une application **HOPEX** peut devenir un élément de traitement dans **HOPEX Privacy Management**.

☛ *Pour plus de détails, voir Gérer les éléments de traitement.*

Ainsi vous pouvez utiliser une application pour créer un élément de traitement sous un traitement existant.

Pour créer des éléments de traitement à partir d'applications :

1. Dans le menu de navigation sélectionnez **Intégration > Applications**.
2. Sélectionnez une application dans l'arbre de gauche et glissez-la dans l'arbre de droite ***sous un département spécifique***.
   S'il n'y a pas de traitement juste en dessous du département voulu, un assistant de création de traitement apparaît. L'élément de traitement est créé sous ce traitement.

DÉFINIR L'ENVIRONNEMENT DE PRIVACY

En tant que responsable de la confidentialité, vous devez définir l'environnement. Il s'agit de pré-définir un certain nombre de listes d'objets (comme les catégories de données, les catégories de personnes concernées).

☛ ***HOPEX Privacy Management*** *fournit des données par défaut qu'il convient de personnaliser. Il est nécessaire de les analyser et de les contextualiser selon les besoins de votre entreprise.*

- ✓ Accéder à l'environnement de Privacy
- ✓ Définir les catégories de données
- ✓ Définir les catégories de personne concernée
- ✓ Définir les activités sensibles
- ✓ Définir des garanties de transfert
- ✓ Définir les autorité de contrôle
- ✓ Définir l'adéquation Pays
- ✓ Définir les mesures de sécurité
- ✓ Définir les technologies
- ✓ Définir les archives physiques

ACCÉDER À L'ENVIRONNEMENT DE PRIVACY

Pour visualiser et modifier les éléments clés de votre environnement :

- Dans le menu de navigation, cliquez sur **Éléments clés**.

Les éléments les plus importants à définir sont les suivants :

- Définir les catégories de données
- Définir les catégories de personne concernée.

Sous les éléments clés RGPD, vous avez également accès aux informations suivantes :

- Définir les activités sensibles
- Définir des garanties de transfert
- Définir les autorité de contrôle
- Définir les mesures de sécurité
- Définir l'adéquation Pays

DÉFINIR LES CATÉGORIES DE DONNÉES

Les catégories des données représentent les catégories de données à caractère personnel.

Il est important de définir correctement les catégories de données pour ensuite décrire les traitements. Vous pouvez également créer des sous-catégories de données.

Pour définir les catégories de données :

1. Dans le menu de navigation, cliquez sur **Éléments clés > Catégories de données**.
2. Identifiez les catégories de données à caractère personnel les plus couramment utilisées dans vos activités métier.

Ci-dessous figurent quelques exemples de catégories de données :

- Identification : nom, adresse, et numéro de carte d'identité
- Médicales : groupe sanguin, état de santé physique
- Données biométriques : Empreintes, reconnaissance vocale
- Données sensibles : race, ethnie, nationalité

Vous pouvez définir :

- la **Période de conservation** : valeur par défaut qui fait référence à la durée de conservation par défaut de ce type de données par l'organisation. Cette période de temps doit être limitée à ce qui est nécessaire pour les finalités pour lesquelles les données à caractère personnel sont traitées.

  ☛ *Cette valeur par défaut donne une indication moyenne de ce que peut être la période de conservation réelle. La période de conservation*

doit être redéfinie sur les traitements, puisqu'elle dépend du contexte et de l'objectif de l'utilisation des données.

Pour plus de détails, voir Spécifier la période de conservation sur un traitement.

- l'**Échelle de risque**: niveau de risque par défaut associé à la catégorie de données (par exemple « élevé » pour les données financières).

  ☛ *Le risque est considéré du point de vue de la personne concernée. Il fait référence à ce qui pourrait se passer en cas de perte, vol ou non disponibilité des données.*

- si la catégorie de données correspond à des **Données sensibles**.

Pour définir une sous-catégorie de données :

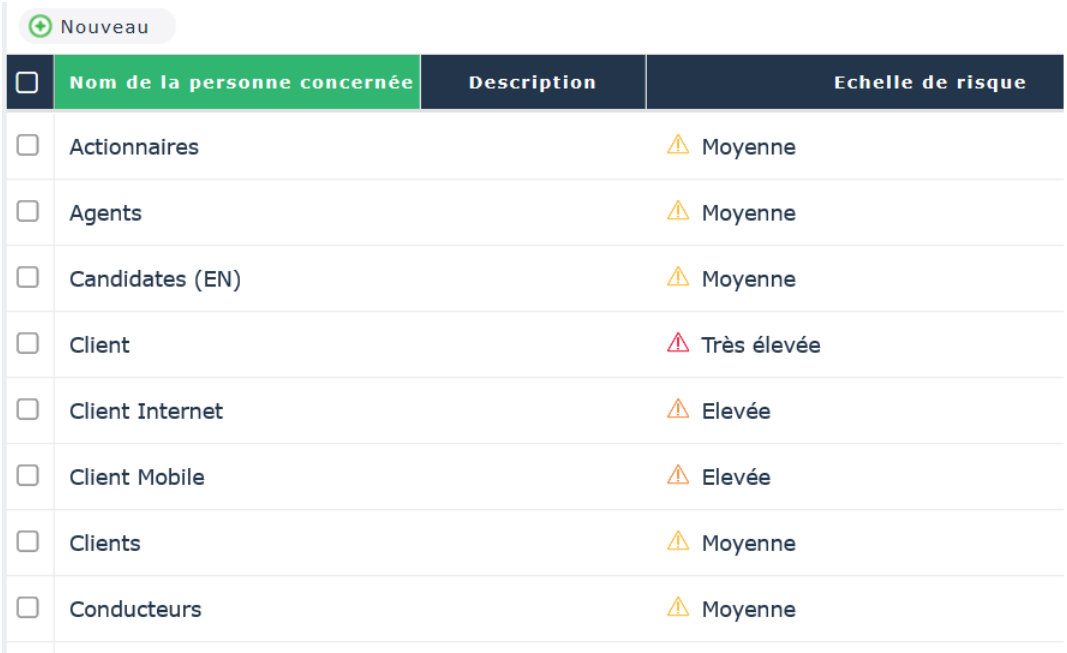
1. Dans la fenêtre de propriétés d'une catégorie de données, dépliez la section **Catégories spécialisées.**
2. Créez une catégorie ou reliez une catégorie existante.

DÉFINIR LES CATÉGORIES DE PERSONNE CONCERNÉE

📖 *Une catégorie de personne concernée est un type de partie prenante qui interagit avec votre organisation dans l'environnement d'entreprise (par exemple un client du secteur privé, un fournisseur).*

Pour définir les catégories de personnes concernées :

1. Dans le menu de navigation, cliquez sur **Éléments clés > Catégories de personnes concernées**.
2. Identifiez toutes les catégories de personnes impliquées dans les traitements réalisés par l'entreprise (par exemple : employés, clients, etc.).
3. Modifiez la valeur par défaut de **Échelle de risque** si nécessaire.



DÉFINIR LES ACTIVITÉS SENSIBLES

📖 *Une activité sensible est une activité dont l'impact global sur le risque du traitement est important.*

Pour définir les activités sensibles :

- Dans le menu de navigation, cliquez sur **Éléments clés > Activités sensibles**.

HOPEX Privacy Management fournit un ensemble prédéfini d'activités sensibles que vous pouvez éditer selon vos propres besoins, par exemple :

- Traitement automatisé de données sensibles
- Traitement à grande échelle de données sensibles

  ☛ *Le groupe de travail Article 29 recommande de prendre en considération les facteurs suivants pour déterminer si le traitement est mené à grande échelle :*

  - *La quantité de personnes concernées, en nombre ou en pourcentage de la population ;*
  - *le volume de données et/ou l'éventail des données traitées*
  - *la durée, ou l'aspect permanent du traitement des données*
  - *l'étendue géographique du traitement*
  - *La surveillance systématique à grande échelle de zones publiques*
- Profilage

  ☛ *Le profilage comprend toute forme de traitement automatisé de données à caractère personnel dont le but est d'évaluer, analyser, ou prédire le comportement des personnes concernées.*

L'**Échelle de risque** des activités sensibles fournies par défaut est « Élevée ».

DÉFINIR DES GARANTIES DE TRANSFERT

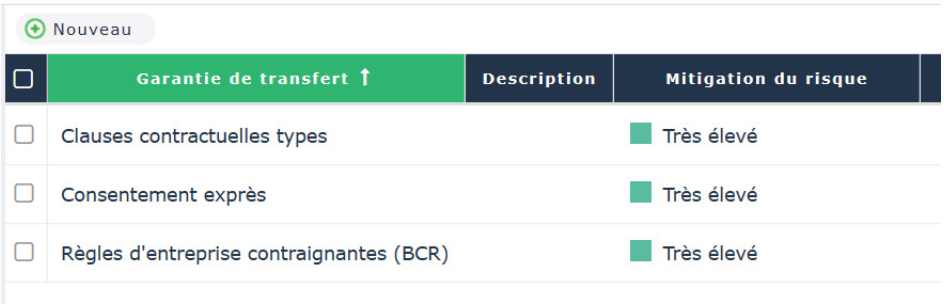
Vous devez vous assurer que les transferts de données sont légitimes et licites.

Les transferts de données hors de l'UE sont par défaut considérés comme étant illicites Toutefois des dérogations existent si des garanties de transfert sont appliquées.

> 🕮 *Les garanties sont des mesures prises pour assurer la légitimité des flux de données. Les garanties s'appliquent aux transferts seulement.*

Pour définir des garanties de transfert :

- Dans le menu de navigation, cliquez sur **Éléments clés > Sécurisation des transferts**.



Les garanties de transfert les plus courantes sont les suivantes :

- Les règles d'entreprise contraignantes (BCR) : code de conduite interne adopté par les multinationales pour permettre les transferts entre différentes branches de l'organisation (utiles dans le cadre des transferts de données inter-groupe).
- Clauses contractuelles types
- Consentement exprès

Pour chaque garantie, vous pouvez indiquer le niveau de **Mitigation** (par défaut, « Très élevé »).

DÉFINIR LES AUTORITÉ DE CONTRÔLE

> 🕮 *Une autorité de contrôle est une autorité publique établie par un état membre. Elle peut être contactée par l'entité juridique dans le but de, par exemple, notifier une violation de données ou faire un retour concernant la DPIA d'un traitement.Elle s'assure que la réglementation en matière de protection des données s'applique. Elle peut demander de la documentation ou des preuves.*

Pour accéder aux autorités de contrôle :

- Dans le menu de navigation, cliquez sur **Éléments clés > Autorités de contrôle**.

L'objectif de cette section est de fournir les informations de contact pour chacune des autorités de contrôle en Europe.

Cette liste est pré-remplie et vous pouvez l'enrichir avec d'autres autorités de contrôle si nécessaire.

Les informations suivantes sont fournies pour chaque autorité de régulation :

- **E-mail**
- **Pays**
- **URL**: adresse du site web

DÉFINIR L'ADÉQUATION PAYS

A propos du concept d'adéquation pays

L'Union Européenne distingue trois catégories de pays :

Pays	Législation	Exigence
UE	RGPD	Aucune garantie requise
Hors UE	Législation en matière de protection de données équivalente à RGPD	Aucune garantie requise
Hors UE	Pas de législation en matière de protection des données	***Des garanties doivent être appliquées***

☛ *Pour plus de détails sur les garanties, voir Définir des garanties de transfert.*

Accéder aux informations concernant l'adéquation pays

Pour accéder aux informations concernant l'adéquation pays :

- Dans le menu de navigation, cliquez sur **Éléments clés > Adéquation RGPD Pays**.

Cette section fournit la liste des pays ainsi que des informations concernant le niveau d'adéquation de la législation du pays en matière de protection des données. Ces informations sont fournies par la Commission Européenne et sont régulièrement mises à jour.

Usage des informations concernant l'adéquation pays

Lorsque vous décrivez un transfert de données existant dans la page de propriété du traitement, le niveau de risque associé au transfert est automatiquement calculé en fonction du niveau d'adéquation pays.

☛ *Pour plus de détails sur les flux de données, voir Spécifier les transferts de données sur un traitement.*

En outre, ces informations peuvent vous guider au moment d'identifier les transferts nécessitant l'adoption de garanties spécifiques (par exemple, les règles d'entreprise contraignantes, les clauses contractuelles types, le consentement).

DÉFINIR LES MESURES DE SÉCURITÉ

Dans le cadre du RGPD, le responsable de traitement et le sous-traitant doivent mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées pour se prémunir contre la destruction accidentelle ou illicite, la modification, la divulgation ou l'accès non autorisé aux données à caractère personnel.

Pour accéder aux mesures de sécurité et les définir :

- Dans le menu de navigation, cliquez sur **Éléments clés > Mesures de sécurité**.

Les mesures de sécurité peuvent avoir pour type :

- **Mesures techniques**

  Exemples : Partitionnement des données, reprise d'activité, anti-virus, pare-feu

- **Mesures organisationnelles**

  Exemples : Politiques et procédures, assignation de rôles spécifiques, maintenance du matériel

- **Système de certification**

  Exemple : ISO 27001, ISO 27018

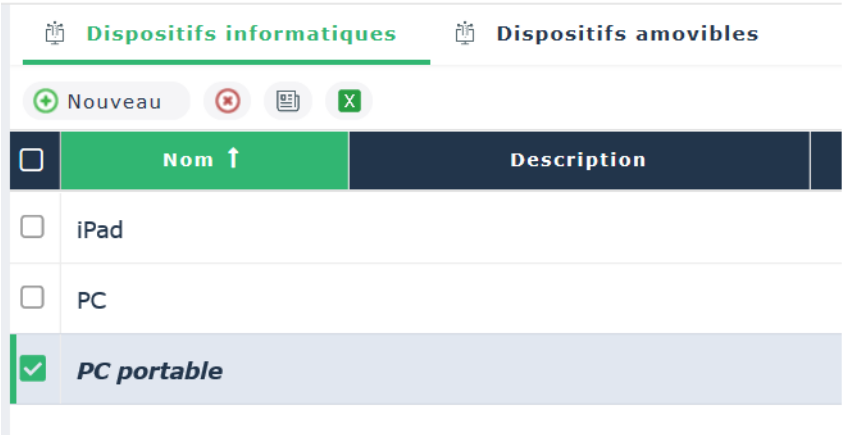
  ☛ *Les mesures de sécurité s'appliquent aux traitements. Les mesures de sécurité s'appliquant aux transferts s'appellent des garanties. Pour plus de détails, voir Définir des garanties de transfert.*

DÉFINIR LES TECHNOLOGIES

Pour gérer les technologies :

- Dans le menu de navigation, cliquez sur **Éléments clés > Technologies**.

Vous pouvez ajouter des dispositifs informatiques ou amovibles.



Dispositifs informatiques

Un ordinateur est un matériel qui peut héberger et exécuter un logiciel. Conjointement avec les applications qu'il héberge, il fournit les services d'information et de données.

`Exemples : Ordinateur portable, PC, iPad.`

Dispositifs amovibles

Cette liste permet de détailler les dispositifs amovibles utilisés dans le cadre de ce traitement.

`Exemples : DVD, clé USB.`

DÉFINIR LES ARCHIVES PHYSIQUES

Une archive physique correspond aux locaux dans lesquels l'historique des archives est conservé.

Pour détailler les archives physiques :

- Dans le menu de navigation, cliquez sur **Éléments clés > Archives physiques**.

La description des archives physiques comprend les informations suivantes :

- Pays
- Adresse
- Description

DÉFINIR L'ORGANISATION

En tant que ***Responsable de la confidentialité***, vous devez définir l'organisation de manière à ce que les membres de l'équipe RGPD puissent réaliser leur mission.

Vous devez créer :

- entités juridiques
- départements

  ☛ *Voir Créer des entités juridiques et des départements.*

  ☛ *Vous pouvez également réutiliser les acteurs existants dans Architecture d'Entreprise pour créer les organisations. Voir Transformer des acteurs EA d'HOPEX en organisations.*

  ☛ *Il est obligatoire de créer des entités et départements. Sans cela, vous ne pourrez pas créer de traitements.*

Vous pouvez créer :

- Des tiers

  ☛ *Voir Gestion des tierces parties.*
- Des documents de politique interne

  ☛ *Voir Gérer les documents de politique interne.*
- L'organigramme des DPO

  ☛ *Voir Visualiser l'organigramme des DPO.*

CRÉER DES ENTITÉS JURIDIQUES ET DES DÉPARTEMENTS

☛ *Il est obligatoire de créer des entités et départements. Sans cela, vous ne pourrez pas créer de traitements.*

A propos des entités et des départements

Une entité juridique est une entreprise ou organisation qui a des droits et obligations juridiques.

Dans **HOPEX Privacy Management**, une « HQ Entity » est créée par défaut. Cette entité représente l'entité siège, dans le cas où plusieurs entités coexistent dans le référentiel.

Vous pouvez créer d'autres entités juridiques (qui ne peuvent être considérées comme le siège, puisqu'il ne peut y avoir qu'une entité faisant office de siège).

☛ *Pour plus de détails sur les entités, voir Définir les propriétés des entités.*

Vous devez créer des départements à relier aux entités juridiques.

☛ *Pour plus de détails sur les départements, voir Gérer les départements.*

Créer une entité juridique

Vous pouvez avoir besoin de créer des entités juridiques autres que l'entité « siège ».

Pour créer une entité juridique :

1. Dans le menu de navigation, cliquez sur **Organisation > Entités juridiques & DPO**.
2. Cliquez sur **Nouveau** pour créer une entité.

☛ *Une entité porte le nom d' « organisation » lors de sa création. D'un point de vue technique, les entités juridiques, les établissements et les départements sont des objets de type « organisation ».*

☛ *Pour plus de détails sur les entités, voir Définir les propriétés des entités.*

Créer des départements

Pour créer un département :

1. Dans le menu de navigation cliquez sur **Organisation > Départements**.
2. Cliquez sur **Nouveau** et dans la fenêtre qui apparaît sélectionnez une **Entité juridique**.

☛ *Il est nécessaire de spécifier l'entité juridique qui gère le département que vous êtes en train de créer.*

Peupler les entités juridiques et les départements

Après avoir créé les entités juridiques et les départements, vous devez les peupler avec des utilisateurs. Cela vous permettra de définir les droits d'accès et de visibilité appropriés.

Vous devez également être relié à un département pour pouvoir créer un traitement

Pour ce faire, voir

- Définir les propriétés des entités
- Gérer les départements

DÉFINIR LES PROPRIÉTÉS DES ENTITÉS

Pour définir des informations sur une entité :

1. Dans le menu de navigation de **HOPEX Privacy Management** , cliquez sur **Organisation > Entités juridiques & DPO**.
2. Sélectionnez une entité.

Propriétés générales d'une entité

La valeur du **Statut** de l'entité s'affiche dans la partie supérieure droite de la fenêtre de propriétés :

- « Opérationnel » : l'entité a été créée et validée par le DPO/l'équipe RGPD
- « Candidat » : l'entité a été créée par une personne qui n'a pas les droits appropriés ; elle doit être validée par le DPO ou l'équipe RGPD
- « Obsolète » : l'entité n'existe plus

> ☛ *Le statut est disponible sur tous les concepts **HOPEX Privacy Management**.*

La page de propriétés donne la possibilité de décrire en détail l'entité juridique.

- **Nom de l'entité juridique**
- **Acronyme**
- **DPO**: qui est le DPO de l'entité juridique
- **Reporting au DPO** : qui est le DPO principal au sein de la hiérarchie des DPO.

  > ☛ *Il est nécessaire de remplir ce champ sur les entités afin de pouvoir afficher les organigrammes des DPO. Pour plus de détails, voir Visualiser l'organigramme des DPO.*
- **Siège du groupe** : indique si l'entité juridique représente le siège (lecture seule)

  > ☛ *Seule l'entité juridique créée par défaut est considérée comme le siège.*
- **UE** : indique si l'entité juridique est située dans l'Union Européenne ou non (lecture seule).

Gérer les établissements

> 🕮 *Un établissement correspond à la localisation (site) d'une entité juridique.*

Pour plus de détails, voir Définir les établissements.

Gérer les représentants nationaux

> 🕮 *Un représentant national est un représentant de l'entité juridique dans l'un des états membres. Une entité juridique n'appartenant pas à l'Union Européenne doit nommer des représentants dans chaque état membre dans lequel l'entité traite des données à caractère personnel.*

Par conséquent, des représentants doivent être nommés lorsque :

- le siège de l'entité se situe hors de l'Union Européenne, et
- l'entité traite des données de personnes dans l'Union Européenne.

Si ce n'est pas le cas, il n'est pas nécessaire de nommer des représentants nationaux.

Le représentant national agit pour le compte du responsable du traitement ou du sous-traitant en ce qui concerne leurs obligations dans le cadre de RGPD.

Pour spécifier les représentants nationaux d'une entité :

❱ Dans la fenêtre de propriétés de l'entité, sélectionnez l'onglet **Représentants nationaux**.

Pour chaque représentant vous pouvez spécifier :

- La **Couverture UE**: quelle partie d'Europe est couverte par le représentant national (par exemple Tous Pays de l'UE).
- La **Date du dernier audit** : date à laquelle le représentant national a été audité par l'entité juridique.

Gérer les accords contractuels

Pour spécifier les accords contractuels applicables à une entité :

❱ Dans la page de propriétés, sélectionnez l'onglet **Accord contractuels**.

Cette section affiche la liste des accords contractuels existants que l'entité juridique a signé avec des tiers.

Un accord contractuel peut être spécifié dans le contexte d'un traitement lorsqu'un tiers est impliqué. Pour plus de détails, voir Gestion des tierces parties.

Les informations suivantes peuvent être fournies sur un accord contractuel :

- **Nom du Contrat**
- **Id de référence** : peut être défini dans un autre outil (SAP par exemple)
- **Périmètre du contrat** : permet de spécifier les entités juridiques et les départements couverts par le contrat.
- **Date d'expiration**
- **Clause spécifique RGPD** : permet de spécifier si le contrat contient des clauses spécifiques à la protection des données
- **Sous-traitance** : permet d'indiquer si le contrat autorise la tierce partie à sous-traiter ses services.

> ☛ *Vous pouvez indiquer si l'accord peut être audité.*

Gérer les utilisateurs

Pour assigner des utilisateurs à une entité juridique :

1. Dans le menu de navigation cliquez sur **Organisation > Entités juridiques & DPO**.
2. Dans la fenêtre de propriétés de l'entité juridique, sélectionnez l'onglet **Utilisateurs** et ajoutez les utilisateurs qui conviennent.

Cette section permet de relier les utilisateurs qui doivent pouvoir accéder aux informations spécifiques à l'entité juridique courante, par exemple à ses traitements.

Les utilisateurs assignés ont une permission de lecture/écriture sur les objets associés à l'entité juridique. Voir aussi : Gérer la visibilité des traitements.

☛ *Si aucun utilisateur spécifique n'est listé, tous pourront visualiser les traitements de l'entité juridique.*

GÉRER LES DÉPARTEMENTS

☛ *Pour créer un département, voir Créer des départements.*

Pour accéder aux départements dans **HOPEX Privacy Management** :

1. Dans le menu de navigation, cliquez sur **Organisation > Départements**.

Dans les pages de propriétés d'un département, vous pouvez :

- Spécifier les caractéristiques générales

  ☛ *Voir Définir les caractéristiques principales d'un département.*

- Définir le DPO ainsi que le correspondant DPO, de manière à pouvoir afficher automatiquement l'organigramme des DPO.

  ☛ *Pour plus de détails, voir Visualiser l'organigramme des DPO.*

- Gérer les utilisateurs

  ☛ *Voir Relier des utilisateurs à un département.*

Définir les caractéristiques principales d'un département

Vous pouvez spécifier les informations suivantes :

- **Nom du département**
- l'**Entité juridique** associée

  ☛ *Il est obligatoire de spécifier une entité juridique sur un département.*

- **Responsable du département**
- **Correspondant DPO** : personne nommée par le DPO pour superviser le département
- **Correspondant support IT**

Relier des utilisateurs à un département

Vous devez ajouter des utilisateurs afin que les propriétaires d'activités puissent créer des traitements.

Pour relier des utilisateurs à un département :

1. Dans les propriétés du département, sélectionnez l'onglet **Utilisateurs**.
2. Reliez les utilisateurs appropriés.

DÉFINIR LES ÉTABLISSEMENTS

Un établissement correspond à la localisation (site) d'une entité juridique.

Vous pouvez décrire les établissements dans les pages de propriétés de l'entité.

Créer un établissement

Pour créer un établissement :

1. Dans le menu de navigation cliquez sur **Organisation > Entités juridiques & DPO**.
2. Dans les propriétés de l'entité juridique, cliquez sur l'onglet **Établissements**.

Vous pouvez définir les informations suivantes sur l'établissement :

- **Nom** de l'établissement
- **Pays**
- **Garanties de transferts**

  📖 *Les garanties sont des mesures prises pour assurer la légitimité des flux de données vers l'établissement.*

  ☛ *Pour plus de détails, voir Définir des garanties de transfert.*
- **Certifications** si applicables

  📖 *Pour plus de détails, voir Spécifier des mesures de sécurité sur un traitement.*

Spécifier l'établissement « siège » de l'entité

Lorsque vous créez plusieurs établissements, vous devez spécifier lequel représente le siège.

Pour indiquer qu'un établissement est le siège :

1. Dans le menu de navigation cliquez sur **Organisation > Entités juridiques & DPO**.
2. Dans la page de propriété de l'entité juridique, sélectionnez l'onglet **Établissements**.

3. Cochez la case **Siège**.

Spécifier le pays d'une entité juridique

Vous pouvez spécifier le pays sur l'établissement siège de l'entité juridique.

Pour spécifier le pays d'une entité juridique :

1. Ouvrez les pages de propriétés de l'entité juridique et sélectionnez l'onglet **Établissements**.
2. Spécifiez le **Pays** pour l'établissement défini comme « siège ».

> ☛ *Il est important d'associer une entité juridique à un pays afin d'illustrer les transferts. Pour plus de détails sur les transferts, voir :*
>
> - *Spécifier les transferts de données sur un traitement*
> - *Carte des flux transfrontaliers*

DÉFINIR UN MODÈLE ORGANISATIONNEL

L'arbre « modèle organisationnel » permet de définir une structure sous les entités juridiques. Il permet également de spécifier les rôles de protection des données impliqués (fonctions).

Définir le modèle organisationnel constitue généralement la première étape dans la mise en place d'un projet de conformité au RGPD.

Pour définir votre modèle organisationnel :

1. Dans le menu de navigation, cliquez sur **Organisation > Modèle organisationnel**.
2. A partir du menu contextuel d'une entité juridique, sélectionnez **Structure** ainsi que l'un des sous-menus suivants :
   - **Nouvelle entité juridique**
   - **Nouveau département**
   - **Nouvelle fonction**

Les fonctions métier permettent d'identifier différents rôles de protection des données.

- Responsable métier
- Responsable de traitement

  📖 *Le responsable de traitement est l'entité qui définit les finalités, conditions et moyens du traitement des données à caractère personnel.*
- Sous-traitant

  📖 *Un sous-traitant est l'entité qui traite des données à caractère personnel pour le compte du responsable de traitement.*
- Responsable de la protection des données

  📖 *Le DPO (Data Protection Officer) ou Responsable de la protection des données travaille de manière indépendante pour s'assurer de la bonne application des textes juridiques concernant les lois de protection des données.*
- Correspondant DPO

  📖 *Un correspondant DPO peut être amené à assister le DPO dans les grandes entreprises.*
- Correspondant informatique

  📖 *Le correspondant informatique est chargé d'assurer le support informatique.*
- Co-responsable du traitement

  📖 *Les co-responsables de traitement peuvent déterminer conjointement les finalités et les moyens du traitement.*

GESTION DES TIERCES PARTIES

La gestion des tierces parties permet de légitimer les transferts de données hors de l'Union Européenne.

> 🕮 *Un tiers est une personne physique ou morale, une autorité publique, un service ou un organisme autre qu'une personne concernée, un responsable de traitement, un sous-traitant et les personnes qui, placées sous l'autorité directe du responsable de traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.*

Pour gérer les tierces parties dans **HOPEX Privacy Management**:

- Dans le menu de navigation cliquez sur **Organisation > Gestion des tierces parties**.

Dans la section vous pouvez spécifier les tiers impliqués dans le traitement des données à caractère personnel.

> ☛ *Vous pouvez trouver ici les mêmes informations que celles qui peuvent être spécifiées sur les entités juridiques. Pour plus de détails, voir Définir les propriétés des entités.*

Le fait de centraliser les données des tiers permet de connaître plus facilement avec qui les données personnelles sont partagées et si les garanties appropriées, comme les clauses contractuelles spécifiques, les codes de conduite, etc, ont été mis en œuvre pour assurer la licité du transfert de données.

VISUALISER L'ORGANIGRAMME DES DPO

Dans **HOPEX Privacy Management**, l'organigramme des DPO montre la hiérarchie des DPO de l'organisation et définit qui rapporte à qui dans l'organisation.

Il permet de communiquer plus rapidement les problèmes à un échelon supérieur, et d'identifier le responsable pour les questions de conformité.

Pour accéder à l'organigramme des DPO :

- Dans le menu de navigation cliquez sur **Organisation > Organigramme des DPO**.

Pour définir un organigramme des DPO, si celui-ci n'est pas disponible :

1. Dans le menu de navigation, sélectionnez **Organisation > Entités juridiques & DPO**.
2. Sélectionnez une entité juridique et dans la fenêtre de propriétés, remplissez les champs suivants :
   - **DPO**
   - **Reporting au DPO** : permet de spécifier les dépendances et d'alimenter l'organigramme des DPO en conséquence.

GÉRER LES DOCUMENTS DE POLITIQUE INTERNE

📖 *Les documents de politique interne permettent de joindre des documents ou de spécifier une URL à utiliser dans le but de fournir des preuves de la responsabilité de l'entreprise.*

Créer des documents de politique interne

Pour créer des documents de politique interne :

- Dans le menu de navigation, cliquez sur **Organisation > Directives & Procédures**.

A la création d'un document de politique interne vous pouvez fournir les informations suivantes :

- **Nom du document**
- **Périmètre** : entité juridique ou département concerné
- **Statut :**
  - Prévu : il est prévu de fournir un document de politique interne mais il n'est pas encore disponible.
  - Non prévu : aucun document n'est disponible
  - En cours : le document est en cours de rédaction
  - Existant : le document est disponible
- **Tag** : vous pouvez associer un tag au document de politique interne de manière à le retrouver facilement.

  ☛ *Pour plus de détails sur les tags, voir Fonctionnalités collaboratives.*

Joindre des documents de politique interne

Pour attacher un document important d'un point de vue du RGPD:

1. Sur le document de politique interne sélectionnez l'onglet **Pièces jointes** et attachez un document métier, ou
2. Sélectionnez l'onglet **Lien** et créez une référence externe qui indique l'URL à utiliser.

Evaluer les documents de politique interne

Dans l'onglet **Evaluation** du document de politique interne, vous pouvez indiquer les informations suivantes :

- **Date de revue**
- **Par** : qui a effectué la revue
- **Conformité** : le réviseur indique le niveau d'efficacité du document par rapport aux exigences du RGPD

GÉRER LES RÉGLEMENTATIONS

HOPEX Privacy Management permet de :

- ✓ Définir des cadres réglementaires et exigences

  📖 *Un cadre réglementaire représente un ensemble de directives contraignantes ou non, définies par un gouvernement dans le cadre d'une loi, par un groupement professionnel sous forme de bonnes pratiques ou en interne par une organisation.*

  📖 *Une exigence est un besoin ou une attente explicitement exprimés, imposés comme contrainte à respecter dans le contexte d'un cadre réglementaire.*
- ✓ Relier ces cadres réglementaires et exigences à des traitements.
- ✓ Visualiser les impacts des réglementations sur les traitements

  ☛ *Voir également Visualiser les impacts des réglementations sur les traitements.*

GÉRER LES CADRES RÉGLEMENTAIRES

📖 *Un cadre réglementaire représente un ensemble de directives contraignantes ou non, définies par un gouvernement dans le cadre d'une loi, par un groupement professionnel sous forme de bonnes pratiques ou en interne par une organisation.*

Accéder aux cadres réglementaires

Pour accéder aux cadres réglementaires :

- Dans le menu de navigation, sélectionnez **Réglementations**.

Une arborescence liste les réglementations, à partir desquelles vous pouvez accéder aux exigences et sous-exigences.

Définir le périmètre d'un cadre réglementaire

Vous pouvez spécifier le périmètre d'un cadre réglementaire en reliant le ***traitement*** au cadre réglementaire.

Pour relier les traitements à un cadre réglementaire :

1. Dans le menu de navigation, sélectionnez **Réglementations**.
2. Ouvrez la page de propriétés du cadre réglementaire.
3. Dans la section **Périmètre**, reliez un traitement.

De cette manière, vous pourrez visualiser le cadre réglementaire dans la page de propriété du traitement (sous la forme d'une arborescence de l'onglet **Réglementations**. Pour plus de détails, voir Visualiser les impacts des réglementations sur les traitements.

☛ *Si les exigences sont reliées au cadre réglementaire, elles apparaîtront également dans l'arborescence mentionnée ci-dessus.*

Décrire les caractéristiques d'un cadre réglementaire

Dans la page de propriétés d'un cadre réglementaire, vous pouvez définir un certain nombre de caractéristiques:

- Code
- Nom
- Date de début d'application
- Date de fin de d'application
- Description détaillée

Vous pouvez également :

- Définir des **Responsabilités** selon la matrice RACI.

  ☛ *RACI est l'acronyme des quatre grandes responsabilités traditionnellement utilisées :*

  - Responsable
  - Autorité
  - Consulté
  - Informé
- Ajouter des **Pièces jointes**

Spécifier les exigences sur un cadre réglementaire

Un cadre réglementaire se compose d'une ou plusieurs exigences.

🕮 *Une exigence est un besoin ou une attente explicitement exprimés, imposés comme contrainte à respecter dans le contexte d'un cadre réglementaire.*

Pour ajouter des exigences :

1. Dans la page de propriétés du cadre réglementaire, dépliez la section **Exigences**.
2. Ajoutez ou créez des exigences.

   ☛ *Les exigences ajoutées au cadre réglementaire apparaîtront dans l'arborescence **Cadre réglementaire** de la page de propriétés du traitement (si l'exigence ou le cadre réglementaire ont été reliés au traitement). Les exigences rattachées apparaîtront également. Pour plus de détails, voir Visualiser les impacts des réglementations sur les traitements.*

GÉRER LES EXIGENCES

Vous devez spécifier une ou plusieurs exigences sur chaque cadre réglementaire.

> 🕮 *Une exigence est un besoin ou une attente explicitement exprimés, imposés comme contrainte à respecter dans le contexte d'un cadre réglementaire.*

Accéder aux exigences

Pour accéder aux exigences :

1. Dans le menu de navigation, sélectionnez **Réglementations**.
   Une arborescence liste les cadres réglementaires.
2. Dépliez les dossiers de cadre réglementaire pour visualiser les exigences associées.

Ajouter des exigences

Pour ajouter des exigences de premier niveau :

1. Dans la page de propriétés du cadre réglementaire, dépliez la section **Exigences**.
2. Reliez des exigences ou créez-en de nouvelles.

Pour ajouter des exigences de second niveau :

1. Dans la page de propriétés du cadre réglementaire, dépliez la section **Exigences**.
2. Ouvrez la page de propriété de l'exigence qui vous intéresse et dépliez la section **Sous-exigences**.
3. Reliez des exigences ou créez-en de nouvelles.

Définir le périmètre d'une exigence

Le périmètre d'une exigence est constitué d'un ou plusieurs traitements.

Pour définir le périmètre d'une exigence :

1. Voir Accéder aux exigences.
2. Dans la page de propriétés d'une exigence, dépliez la section **Périmètre** et reliez un traitement.

De cette manière, vous pourrez visualiser l'exigence dans une arborescence de la page de propriétés du traitement (onglet **Réglementations**). Le cadre réglementaire parent de l'exigence apparaîtra également. Pour plus de détails, voir Visualiser les impacts des réglementations sur les traitements.

Décrire les caractéristiques d'une exigence

Pour définir les caractéristiques d'une exigence :

- Dans la page de propriétés d'une exigence, spécifiez les informations suivantes :
  - **Code** : permet d'identifier l'exigence de manière unique
  - **Exigence parente** : exigence à laquelle l'exigence est rattachée.
  - **Cadre réglementaire**: réglementation à laquelle l'exigence est rattachée.
  - **Priorité** (faible, moyenne, forte)
  - **Émetteur** : organisation qui a publié l'exigence

GÉRER LES TRAITEMENTS

Le traitement est au cœur de **HOPEX Privacy Management**. Il permet à l'organisation de décrire à quelle fin les données personnelles sont utilisées et comment elles sont gérées.

En tant que ***Propriétaire de traitement***, vous êtes en charge de la description détaillée des traitements.

☛ *Pour l'évaluation des traitements par le DPO une fois les traitements décrits, voir Évaluer les traitements.*

☛ *Pour la résolution de problèmes, voir A propos des traitements.*

CONDITIONS PRÉALABLES À LA CRÉATION DE TRAITEMENTS

Le responsable de la confidentialité doit avoir créé l'organisation qui va vous permettre de décrire les traitements. Il convient de réaliser au préalable les points suivants :

- Définir les entités juridiques
- Définir les départements
- Relier les utilisateurs aux entités juridiques et aux départements

Pour plus de détails, voir Définir l'organisation.

CRÉER LES TRAITEMENTS

Vous pouvez créer des traitements directement dans **HOPEX Privacy Management**.

☛ *Voir Créer des traitements dans HOPEX Privacy Management.*

Vous pouvez également créer des traitements :

- en dupliquant un traitement existant

☛ *Voir Créer un traitement par duplication.*

- en réutilisant des processus et applications de l'Architecture d'Entreprise.

☛ *Voir Créer des traitements à partir d'objets HOPEX.*

Créer des traitements dans HOPEX Privacy Management

Pour créer un traitement directement dans **HOPEX Privacy Management** :

1. Dans le menu de navigation sélectionnez **Traitements**.
2. Cliquez sur **Nouveau**.

Si besoin, vous pouvez créer des éléments de traitement. Dans ce cas, il est conseillé :

- dans un premier temps, de décrire le traitement général
- dans un deuxième temps, de créer des éléments de traitement lorsque des différences existent sur certaines parties du traitement.

☛ *Pour plus de détails, voir Gérer les éléments de traitement.*

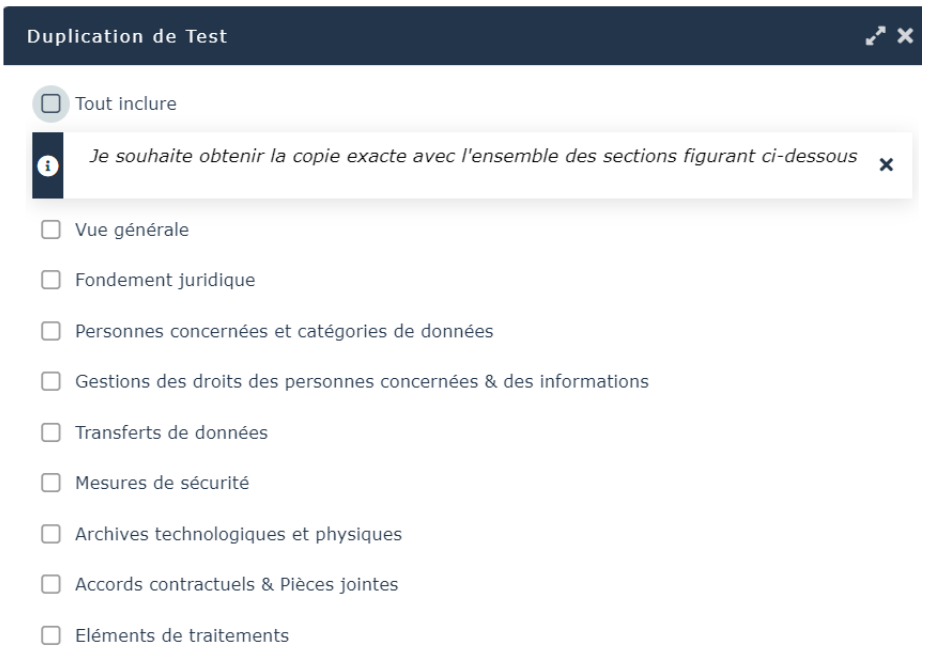
Créer un traitement par duplication

Vous pouvez créer un traitement en dupliquant un traitement existant. Le traitement existant sert en quelque sorte de modèle.

Pour dupliquer un traitement :

1. Dans le menu de navigation sélectionnez **Traitements**.
2. Sélectionnez un traitement.
3. Cliquez sur le bouton ⋮ qui apparaît et sélectionnez **Dupliquer**.

4. Dans l'assistant qui apparaît, sélectionnez les sections que vous voulez dupliquer :
   - Vue générale
     ☛ *Voir Vue globale des traitements.*
   - Fondement juridique
     ☛ *Voir Fondement juridique du traitement.*
   - Personnes concernées et catégories de données
   - Gestion des droits des personnes concernées et des informations
     ☛ *Voir Gestion des droits des personnes concernées et des informations.*
   - Transferts de données
     ☛ *Voir Transferts de données.*
   - Mesures de sécurité
     ☛ *Voir Mesures de sécurité.*
   - Technologiques et archives physiques
     ☛ *Voir Technologies et Archives physiques.*
   - Eléments de traitement
     ☛ *Voir Gérer les éléments de traitement.*



5. Cliquez sur **OK**.

ACCÉDER AUX REGISTRE DES TRAITEMENTS

Accéder aux traitements

Pour accéder aux traitements dans **HOPEX Privacy Management**:

1. Dans le menu de navigation, sélectionnez **Traitements**.
2. Sélectionnez un traitement pour ouvrir sa page de propriétés.

Si votre registre de traitements contient de nombreux traitements, vous pouvez restreindre le périmètre des traitements à afficher. Voir Affiner le périmètre du registre des traitements.

Affiner le périmètre du registre des traitements

Les lois de protection des données personnelles peuvent exiger de tenir à jour deux registre de traitements distincts :

- l'un en tant que responsable de traitement
- l'autre en tant que sous-traitant

HOPEX Privacy Management propose d'utiliser un filtre avancé pour exporter facilement les traitements d'une ou plusieurs entités en fonction du rôle de protection des données.

Pour affiner le périmètre des traitements affichés dans votre registre des traitements :

1. Accédez au registre des traitements
   ☛ *Voir Accéder aux traitements.*
2. En haut de la liste des traitements, cliquez sur bouton **Périmètre du registre**.

3. Spécifiez les **Entités juridiques** qui vous intéressent.

4. Spécifiez le rôle de protection des données:
   - **Responsable de traitement**
   - **Co-responsable du traitement**
   - **Sous-traitant**
5. Cliquez sur **Appliquer**.

La liste des traitements est mis à jour en fonction des critères spécifiés.

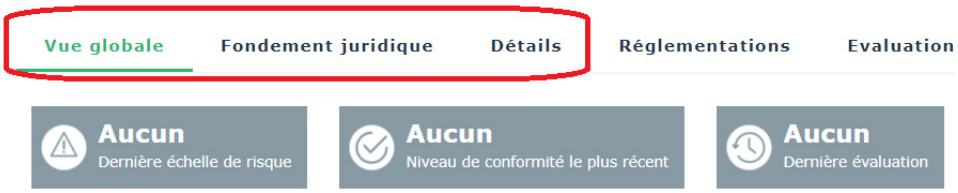
DÉCRIRE LES TRAITEMENTS

☛ *Pour plus de détails sur la création de traitements, voir Créer les traitements.*

☛ *Voir également Accéder aux traitements.*

En tant que propriétaire de traitement, vous pouvez décrire un traitement dans les trois premiers onglets de sa page de propriétés :

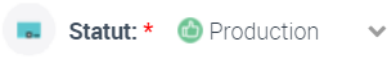
- **Vue globale** : voir Vue globale des traitements.
- **Fondement juridique** : voir Fondement juridique du traitement.
- **Détails** : voir Détails du traitement.



☛ *Les onglets **Évaluation préliminaire** et **DPIA** sont réservés à l'équipe Privacy. Pour plus de détails, voir Évaluer les traitements.*

Visualiser le processus à l'origine du traitement

Un traitement créé à partir d'un processus HOPEX est illustré par une icône représentant un processus à côté du statut du traitement :



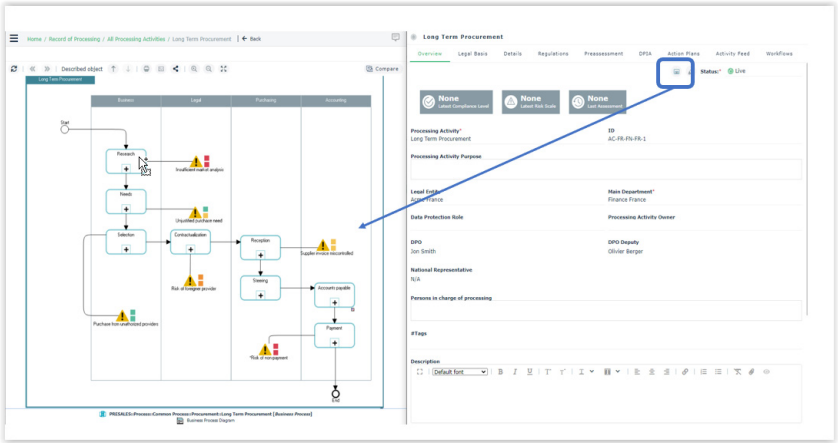
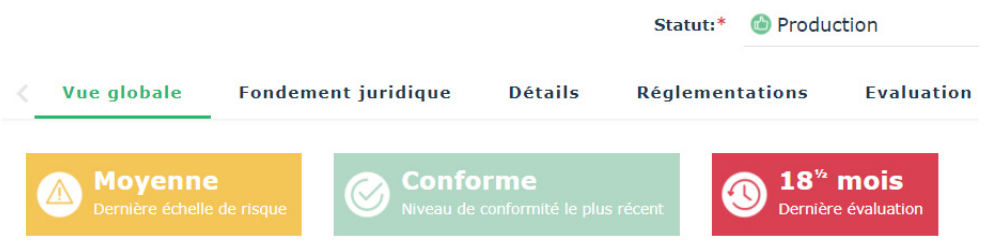


Tableau de bord du traitement

En haut de la page des propriétés vous trouvez un bilan global du traitement.

L'information affichée prend en compte les évaluations réalisées au cours des évaluations préliminaires et des analyses d'impact (DPIA). Ce tableau de bord est vide jusqu'à ce que l'équipe Privacy commence l'évaluation du traitement.

☛ *Pour plus de détails, voir Consulter les rapports et les résultats de la DPIA.*



Vue globale des traitements

Informations supplémentaires à spécifier

La page de propriétés d'un traitement affiche les informations générales suivantes :

- Nom du **Traitement**
- **ID**: identifiant

  ☛ *L'identifiant est automatiquement calculé en fonction des acronymes de l'entité juridique et du département associés.*
- **Finalité du traitement**: permet de saisir du texte libre pour décrire la finalité de votre traitement.

  🕮 *La finalité d'un traitement est l'objectif principal de ce traitement. Exemples : enquête de satisfaction, gestion des clients, surveillance d'un site*
- **Rôle de protection des données**: permet d'indiquer le rôle joué par l'entité juridique
  - « Responsable de traitement »

    🕮 *Le responsable de traitement est l'entité qui définit les finalités, conditions et moyens du traitement des données à caractère personnel.*

    ☛ *Il est obligatoire de spécifier un responsable de traitement.*
  - « Sous-traitant »

    🕮 *Un sous-traitant est l'entité qui traite des données à caractère personnel pour le compte du responsable de traitement.*
  - « Co-responsable du traitement »

    🕮 *Les co-responsables de traitement sont des responsables de traitement qui déterminent conjointement les finalités et les moyens du traitement.*
- **Propriétaire de traitement**

  🕮 *Le propriétaire de traitement fournit une description détaillée du traitement. Il ne participe pas à l'évaluation du traitement.*
- **Détails**: saisissez un commentaire
- **Activités sensibles** : indique quelles opérations menées dans le cadre du traitement sont susceptibles d'influencer le niveau de risque final.

  ☛ *Pour plus de détails, voir Définir les activités sensibles.*
- **Date de début** et **Date de fin**
- **Traitement informatique / Traitement papier** : spécifiez si le traitement inclut des traitements informatiques / papier ou les deux
- **Personnes responsables du traitement** : saisissez manuellement les personnes réellement chargées du traitement

Informations disponibles en lecture seule

Certains champs sont remplis de façon automatique (ils sont en lecture seule) :

- **Entité juridique**
- **Département**
- **DPO**

  ☛ *Le DPO est défini au niveau de l'entité juridique.*

- **Correspondant DPO**

  ☛ *Le DPO est défini au niveau de l'entité juridique.*

- **Représentant National**

  📖 *Un représentant national est un représentant de l'entité juridique dans l'un des états membres. Une entité juridique n'appartenant pas à l'Union Européenne doit nommer des représentants dans chaque état membre dans lequel l'entité traite des données à caractère personnel.*

  ☛ *Ce champ indique le niveau de couverture des pays européens. Pour plus de détails, voir Gérer les représentants nationaux.*

  - « Complet » : tous les représentants des pays européens sont assignés
  - « Partiel » : au moins un représentant national qui couvre un pays européen a été assigné.
  - « Non » : aucun représentant n'a été assigné jusqu'ici.
  - "N/A": l'entité juridique est située en Europe ; il n'est pas nécessaire de spécifier des représentants nationaux.

Participants au traitement

Par défaut, les entités et départements suivants peuvent accéder au traitement :

- l'entité juridique et le département principal définis plus haut dans cette page.
- les entités qui apparaissent dans la page **Détails du traitement**.

  ☛ *Voir Niveaux de détail des traitements.*

Pour définir d'autres participants :

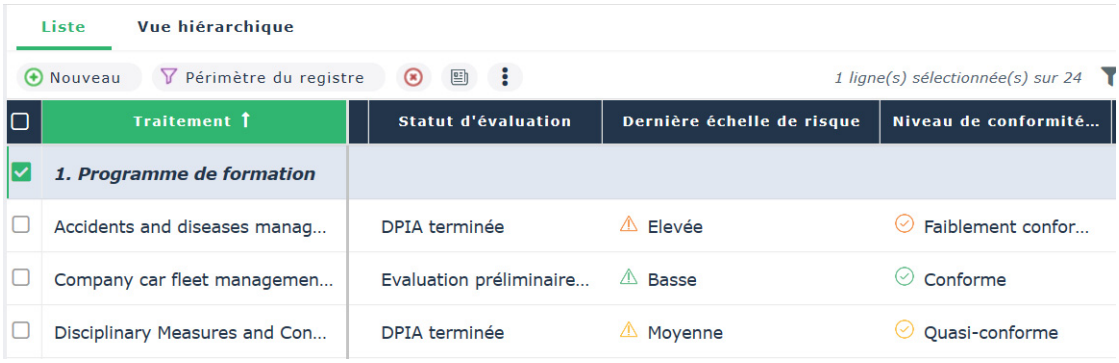
1. Dans la page de propriétés d'un traitement, dépliez la section **Autres participants**.
2. Reliez les éléments suivants :
   - **Entités juridiques**
   - **Départements**

Information calculée

Dans la liste des traitements, les colonnes fournissent des informations calculées basées sur les évaluations (évaluations préliminaires ou DPIA), telles que :

- la date d'évaluation : dernière évaluation réalisée
- le statut d'évaluation : indique si une évaluation a été réalisée
- l'échelle de risque
- Le niveau de conformité final

☛ *Si aucune évaluation n'a été faite, la cellule reste vide.*



Fondement juridique du traitement

Vous devez spécifier le fondement juridique du traitement et fournir en pièce jointe tout document pertinent. Il s'agit du motif juridique qui établit la légitimité du traitement.

Vous devez vous appuyer sur un fondement juridique pour pouvoir traiter des données à caractère personnel.

📖 *Le fondement juridique est ce qui vous autorise à réaliser des traitements.*

Il existe différents fondements possibles pour un traitement. Pour RGPD, ils sont cités à l'article 6. Au moins l'un deux doit s'appliquer lors du traitement de données à caractère personnel.

- **Consentement exprès** : la personne concernée a librement consenti à ce que ses données à caractère personnel soient traitées dans un but spécifique.

📖 *Le consentement est une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des*

données à caractère personnel la concernant fassent l'objet d'un traitement.

Exemple : traitement des données personnelles dans le cadre d'email marketing.

- **Obligation contractuelle** : le traitement est nécessaire dans le cadre de l'exécution d'un contrat.

  Exemple : traitement des données personnelles des employés pour la gestion des salaires.

- **Application du droit** : le traitement est nécessaire pour vous conformer à la loi (cela exclut les obligations contractuelles).

  Exemple : Traitement des données des clients d'une banque afin d'empêcher le blanchiment d'argent.

- **Intérêt vital** : le traitement est nécessaire pour sauver ou protéger la vie d'un individu.

  Exemple : traitement des données de patients dans le cas d'un traitement médical.

- **Intérêt public** : le traitement est nécessaire dans l'exécution d'une tâche d'intérêt public ou l'exercice de fonctions officielles (la tâche ou la fonction doivent avoir un fondement légal bien déterminé).

  Exemple : traitement de données à caractère personnel liées à d'éventuelles condamnations pénales ou infractions, à des fins d'enquête

- **Intérêt légitime** : le traitement est corrélé au service fourni par la mission commerciale. La mission ne peut exister sans le traitement.

  Exemple : traitement des données de visiteurs pour raisons de sécurité.

  ☛ *Si vous sélectionnez **Intérêt légitime** comme fondement juridique, il peut être utile de fournir des informations complémentaires en commentaire. Le fondement juridique nécessite généralement des preuves détaillées de la légitimité du traitement.*

L'équipe Privacy peut évaluer par la suite le **Fondement juridique** à partir des options sélectionnées précédemment par le propriétaire de traitement.

DÉTAILS DU TRAITEMENT

L'onglet **Détails** est central dans la description du traitement.

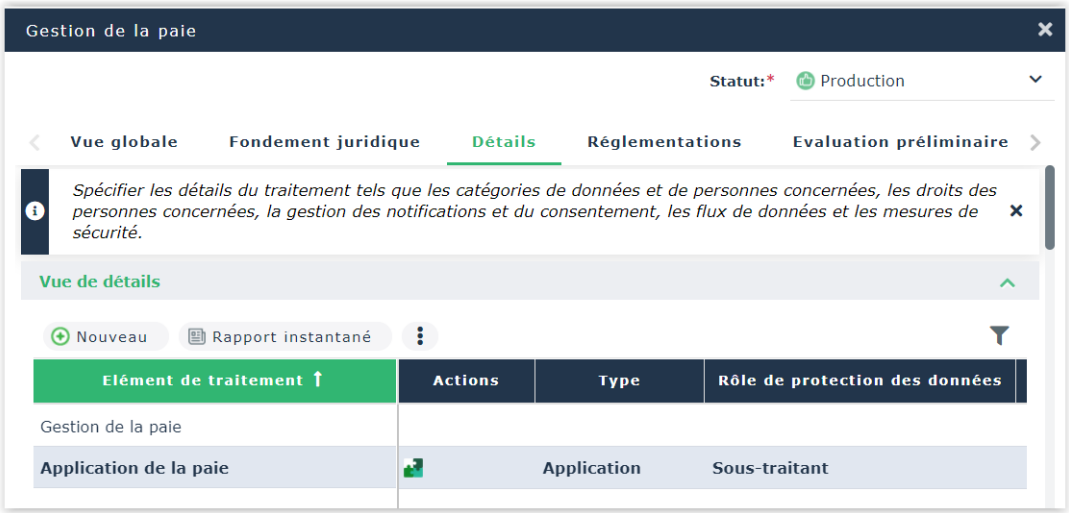
Niveaux de détail des traitements

Tout traitement doit être décrit à un premier niveau général. Il peut en outre être utile de créer des éléments de traitement lorsque vous faites appel à une application ou à un sous-traitant pour l'exécution d'un traitement.

Dans ce cas vous devez procéder de la façon suivante :

- commencez par décrire le traitement au niveau général
- (Optionnel) créez des éléments de traitement et saisissez les informations qui diffèrent du traitement général.

☛ *Pour plus de détails, voir Créer un élément de traitement.*



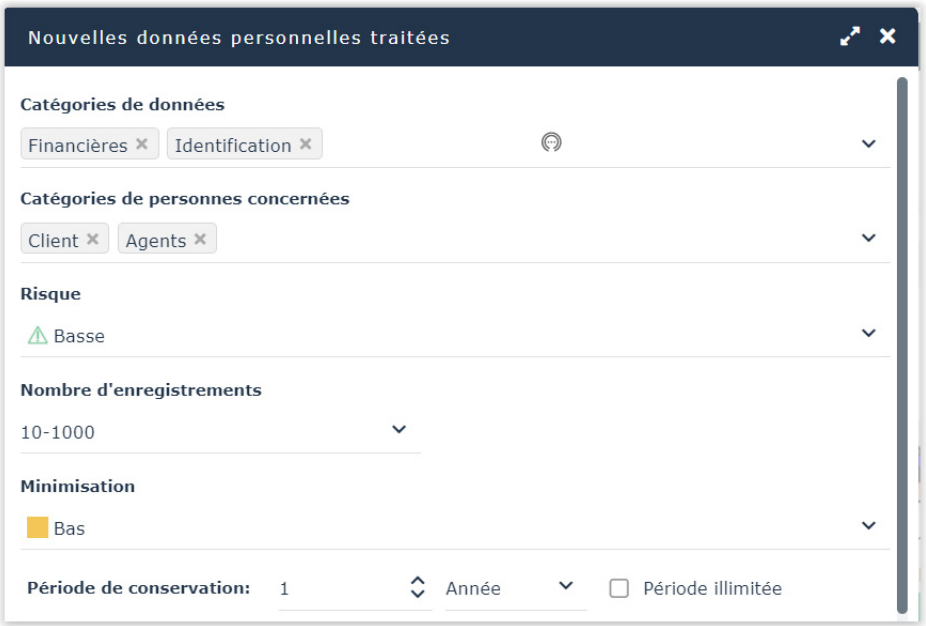
Pour le traitement général, vous pouvez saisir les informations suivantes.

- Données à caractère personnel traitées
- Gestion des droits des personnes concernées et des informations
- Transferts de données et Mesures de sécurité
- Technologies et Archives physiques
- Accords contractuels et autres pièces jointes

Données à caractère personnel traitées

Pour créer des données à caractère personnel :

1. Voir Accéder aux traitements.
2. Ouvrez les propriétés du traitement et sélectionnez la page **Détails**.
3. Dans la section **Données personnelles traitées**, cliquez sur **Nouveau**.



Vous pouvez spécifier les informations suivantes :

- **Catégories de données**

  ☛ *Dans la liste sont proposées également les catégories spécialisées d'une catégorie de données (qui constituent des sous-catégories).*

- **Personnes concernées**
- **Nombre d'enregistrements** : correspond au nombre de personnes concernées impliquées dans votre registre de traitement.
- **Minimisation**

  🕮 *La minimisation est un principe selon lequel les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.*

  ☛ *Voir Qualifier la minimisation.*

- **Période de conservation**

  ☛ *Voir Spécifier la période de conservation sur un traitement.*

Qualifier la minimisation

La minimisation est un principe important dans le Règlement général sur la protection des données de l'Union européenne ainsi que dans d'autres lois sur la protection des données.

Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. De plus, les données collectées pour une finalité ne peuvent être réutilisées sans un nouveau consentement.

Valeurs de minimisation possibles	Signification
Bas/Très bas	Trop d'informations sont utilisées
Élevée	Les informations utilisées correspondent strictement au besoin

L'équipe Privacy peut définir un niveau de conformité dans la section Données personnelles traitées, sur la base des informations saisies par le propriétaire de traitement :

- Dans le champ **Niveau de conformité Minimisation des données**, sélectionnez une valeur dans le menu déroulant.

Visualiser le risque calculé

A la création de données à caractère personnel, le niveau de **Risque** est automatiquement calculé à partir de l'échelle de risque la plus haute spécifiée par le responsable de la confidentialité dans la section **Éléments clés** (pour les catégories de données et les catégories de personnes concernées).

> 🕮 *Un risque représente un risque relatif à la protection des données qui doit être identifié et évalué au cours d'un DPIA.*
>
> ☛ *Pour plus d'informations sur l'échelle de risque initiale définie par le responsable de la confidentialité, voir Définir les catégories de données et Définir les catégories de personne concernée.*

Spécifier la période de conservation sur un traitement

Spécifier une période de conservation sur un traitement est essentiel. La période de conservation effective peut être déterminée par des lois locales.

Lorsque la période de conservation effective a été spécifiée, elle est comparée à la période de conservation visée. La couleur de l'icône indique le degré de conformité avec la période visée.

> 🕮 *La période de conservation visée correspond à la période de conservation par défaut la plus faible des catégories de données sélectionnées.*

Gestion des droits des personnes concernées et des informations

Cette section est disponible sous l'onglet **Détails** de la page de propriétés d'un traitement.

Dans cette section vous pouvez spécifier les informations suivantes :

- Les droits garantis par le traitement pour les personnes concernées

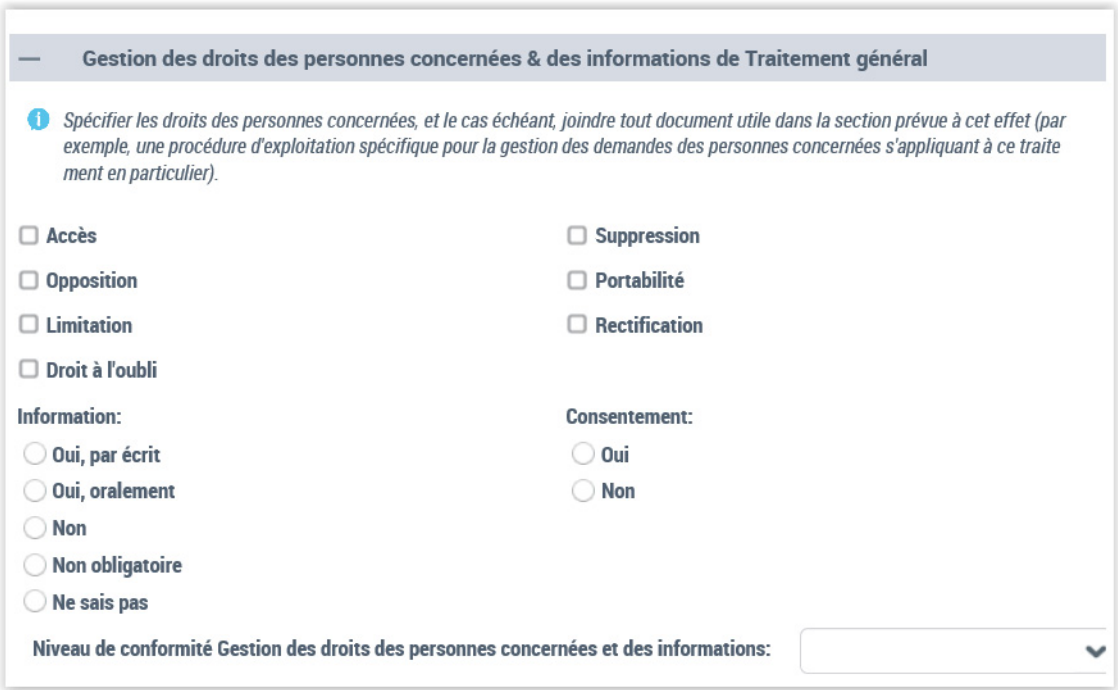
  ☛ *Voir Spécifier les droits des personnes concernées sur un traitement pour plus d'informations.*

- comment l'information est gérée (par écrit, oralement, non obligatoire).

  ☛ *Pour visualiser un rapport sur la gestion des informations, voir Informations.*

- si un consentement a été fourni ou non

  📖 *Le consentement est une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.*



Spécifier les droits des personnes concernées sur un traitement

Vous pouvez spécifier les droits pris en compte dans votre traitement.

☛ *Au moins un des droits suivants doit être sélectionné.*

- **Accès**

  🕮 *Le droit d'accès permet aux personnes concernées d'accéder aux données à caractère personnel les concernant et que le responsable de traitement détient.*

- **Objet**

  ☛ *La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant.*

- **Limitation**

  ☛ *La personne concernée devrait avoir le droit d'obtenir du responsable du traitement la limitation du traitement.*

- **Droit à l'oubli**

  🕮 *Le droit à l'oubli est également appelé Droit à l'effacement. Il autorise la personne concernée à faire supprimer ses données à caractère personnel par le responsable de traitement, à stopper la dissémination de ses données, et à interdire leur traitement par des tiers.*

- **Effacement**

  🕮 *Une personne concernée peut avoir le droit de demander à supprimer des données la concernant que vous avez en votre possession.*

- **Portabilité**

  🕮 *La portabilité est l'exigence pour les responsables de traitement de fournir à toute personne concernée une copie de ses données dans un format permettant à un autre responsable de traitement d'en faire usage.*

- **Rectification**

  ☛ *Toute personne concernée devrait pouvoir obtenir du responsable de traitement et dans les meilleurs délais la rectification des données à caractère personnel inexactes la concernant.*

Visualiser les droits des personnes concernées sur vos traitements

En tant que propriétaire de traitement ou d'application, vous pouvez visualiser les droits des personnes concernées sur les traitements dont vous êtes responsable.

HOPEX Privacy Management fournit un rapport pour cela.

Pour avoir une vue générale des droits des personnes concernées :

❱ Dans le bureau du propriétaire de traitement, cliquez sur **Rapports > Droits des personnes concernées**.

Attribuer un niveau de conformité sur les droits des personnes concernées

Par la suite, dans cette section, l'équipe Privacy peut définir un niveau de conformité basé sur les informations mentionnées précédemment. Pour ce faire :

❱ Sélectionnez une valeur dans le menu déroulant **Niveau de conformité Minimisation des données**.

Transferts de données

> 🕮 *Dans le cadre d'une loi sur la protection des données personnelles, un transfert de données est un transfert ou une copie de données à caractère personnel.*

Cette section vous permet de créer les transferts de données spécifiques à votre traitement.

Pour créer des transferts de données et des mesures de sécurité sur un traitement :

1. Ouvrez la page de propriétés du traitement.
2. Sélectionnez l'onglet **Détails**.

Spécifier les transferts de données sur un traitement

A la création d'un transfert, vous devez spécifier :

- le nom du transfert
- le destinataire (entités juridiques et sous-traitants)

  > ☛ *Le pays du destinataire est calculé automatiquement à partir de l'établissement principal de l'entité.*

- l'émetteur
- les catégories de données et les personnes concernées

  > 🕮 *Les catégories des données sont utilisées dans le but de regrouper différentes données à caractère personnel. Voir Définir les catégories de données pour plus d'informations.*

  > 🕮 *Une catégorie de personne concernée est un type de partie prenante qui interagit avec votre organisation dans l'environnement d'entreprise (par exemple un client du secteur privé, un fournisseur). Voir Définir les catégories de personne concernée pour plus d'informations.*

- les garanties appliquées

  > 🕮 *Les garanties sont des mesures prises pour assurer la légitimité des flux de données. Les garanties s'appliquent aux transferts seulement.*
  >
  > *Pour plus de détails, voir Définir des garanties de transfert.*

- si les données sont externalisées
- si les données sont vendues/achetées

Attribuer un niveau de conformité aux mesures de sécurité

Par la suite, dans cette section, l'équipe Privacy peut définir un niveau de conformité basé sur les informations mentionnées précédemment. Pour ce faire :

1. Sous l'onglet **Détails** de la page du traitement, faites défiler la page jusqu'à la section correspondant aux mesures de sécurité.
2. Sélectionnez une valeur dans le champ **Niveau de conformité Mesures de sécurité**.

Mesures de sécurité

Spécifier des mesures de sécurité sur un traitement

Pour créer un groupe de mesures de sécurité applicables à un traitement :

1. Voir Accéder aux traitements.
2. Dans la page de propriétés du traitement, sélectionnez l'onglet **Détails**.
3. Faites défiler la page jusqu'à la section **Mesures de sécurité** et sélectionnez l'onglet qui correspond au type de mesure de sécurité :
   - Mesures techniques
   - Mesures organisationnelles
   - Systèmes de certification
4. Cliquez sur **Nouveau**.
5. Dans le champ **Sujet** saisissez un nom général pour le groupe de mesures de sécurité.
6. A partir de la liste déroulante **Mesures de sécurité**, sélectionnez les mesures de sécurité individuelles dont vous avez besoin pour votre traitement.

   ☛ *Pour plus d'informations sur ces mesures de sécurité, voir Définir les mesures de sécurité.*
7. Saisissez une description.
8. Sélectionnez le niveau de **Mitigation** attendu pour ce groupe de mesures de sécurité.

Attribuer un niveau de conformité aux mesures de sécurité

Par la suite, dans cette section, l'équipe Privacy peut définir un niveau de conformité basé sur les informations mentionnées précédemment.

Pour ce faire :

1. Sous l'onglet **Détails** de la page du traitement, faites défiler la page jusqu'à la section concernant les mesures de sécurité.
2. Sélectionnez une valeur dans le champ **Niveau de conformité Mesures de sécurité**.

Technologies et Archives physiques

Cette section vous permet de relier des dispositifs informatiques/amovibles ainsi que des archives physiques propres à votre traitement.

Pour ajouter des technologies et archives physiques à un traitement :

1. Ouvrez la page de propriétés du traitement.
2. Sélectionnez l'onglet **Détails** et faites défiler la page jusqu'à la section **Technologies et archives physiques**.

Vous pouvez relier des objets des catégories suivantes (qui ont été définis au préalable par le responsable de la confidentialité).

- Dispositif informatique
- Dispositif amovible
- Archive physique

> ☛ *Pour plus de détails, voir Définir les technologies et Définir les archives physiques.*

Accords contractuels et autres pièces jointes

Vous pouvez relier des accords contractuels ou des modèles pour la publication d'informations aux personnes concernées par exemple.

> ☛ *Vous pouvez trouver des modèles dans la documentation **HOPEX Privacy Management** du menu suivant : **Registre des traitements > Ressources et modèles**.*

Pour attacher un accord contractuel :

1. Dans l'onglet **Détails** de la page d'un traitement, dépliez la section **Accords contractuels & autres pièces jointes**.
2. Sélectionnez l'onglet **Accords contractuels**.
3. Cliquez sur **Nouveau**.
4. Remplissez les champs comme il convient :
   - **Nom du Contrat**
   - **Périmètre du contrat**
   - **Date d'expiration**
   - **Clause spécifique** : oui/non
   - **Sous-traitance**: indiquez si le traitement peut faire appel à des sous-traitants.

GÉRER LES ÉLÉMENTS DE TRAITEMENT

Si vous avez besoin d'une vue globale, vous pouvez traiter uniquement le traitement général (ce qui signifie qu'il n'est pas nécessaire de spécifier des éléments de traitement).

Pour plus de détails, voir :

- Créer les traitements
- Décrire les traitements

Cependant, si un traitement implique une application informatique ou un sous-traitant, vous pouvez définir des éléments de traitement afin de le décrire plus finement.

Créer un élément de traitement

Pour créer un élément de traitement :

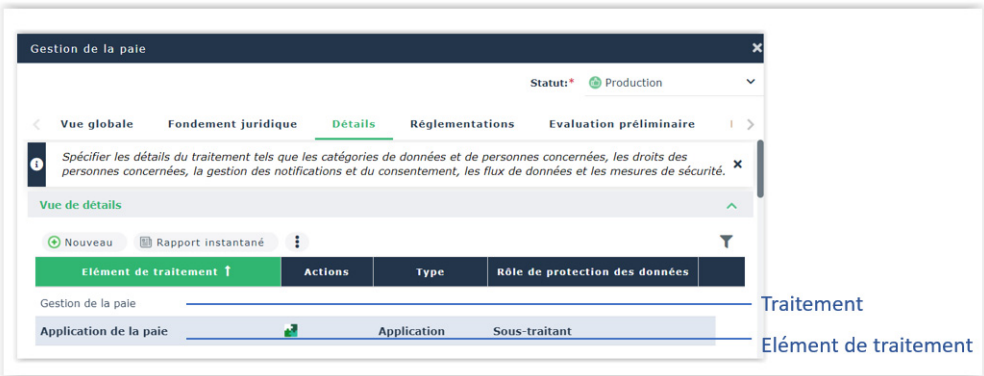
1. Voir Accéder aux traitements.
2. Dans la fenêtre de propriétés d'un traitement, sélectionnez la page **Détails**.
3. Dans la section **Vue de détails**, cliquez sur **Nouveau**.
4. Sélectionnez le type d'élément de traitement.
   - Organisation
   - Tierce partie
   - Application

> ☛ *Pour plus de détails, voir Spécifier un élément de traitement de type « Application ».*

Vous pouvez fournir des informations sur le rôle de protection des données du fournisseur d'application ou de la tierce partie.

Pour décrire l'élément de traitement :

1. Sélectionnez l'élément de traitement créé.
2. Notez que la page de propriétés s'applique à l'élément de traitement.



Spécifier un élément de traitement de type « Application »

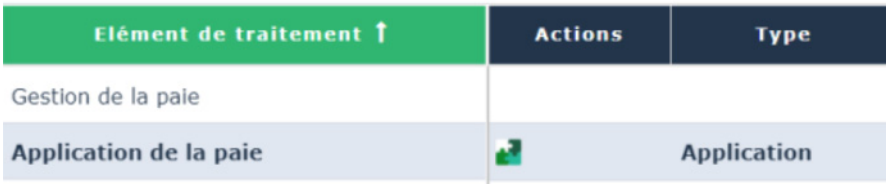
Pour créer un élément de traitement de type « Application » :

1. Créez un élément de traitement.

   ☛ *Voir Créer un élément de traitement.*

2. Dans la liste déroulante **Type**, sélectionnez « Application ».
3. Si des applications d'autres solutions **HOPEX** ont été importées dans **HOPEX Privacy Management**, sélectionnez l'une d'elles dans la liste déroulante correspondante.

4. Cliquez sur **OK**.
5. L'élément de traitement apparaît sous le traitement principal.



Afficher les propriétés de l'application et le site web associé

Les applications provenant d'autres solutions **HOPEX** telles que **HOPEX IT Portfolio Management** sont signalées par la présence d'un icône.

Un lien vers un site web externe est disponible si l'application en question est décrite dans un site web statique.

VISUALISER LES IMPACTS DES RÉGLEMENTATIONS SUR LES TRAITEMENTS

HOPEX Privacy Management vous permet de consulter les réglementations qui s'appliquent à un traitement particulier.

Pour visualiser les réglementations applicables :

- Dans la page de propriété d'un traitement, sélectionnez l'onglet **Réglementations**.

Une arborescence affiche les réglementations et exigences qui s'appliquent au traitement. Cette arborescence est en mode lecture seule.

☛ *Pour visualiser l'arborescence, vous devez avoir au préalable défini de manière adéquate le périmètre (les traitements) des réglementations et exigences à partir de la section **Réglementations**.*

Pour plus de détails, voir :

- *Définir le périmètre d'un cadre réglementaire*
- *Définir le périmètre d'une exigence*

UTILISER LE WORKFLOW DES TRAITEMENTS

Un workflow standard vous permet de gérer le cycle de vie des traitements.

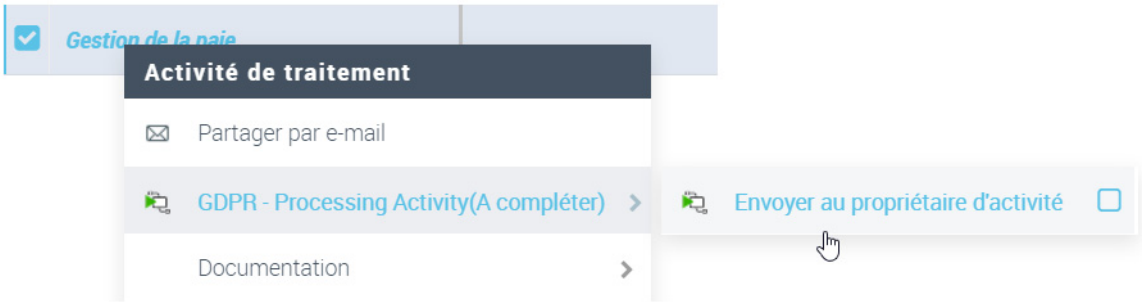
Le responsable de la confidentialité crée un traitement. Il demande au propriétaire de traitement d'en faire une description. Une fois le traitement décrit, le responsable de la confidentialité peut valider le traitement. Il est alors possible de réaliser une évaluation préliminaire ou une DPIA.

☛ *Pour plus de détails sur la création de DPIA, voir Quelles sont les possibilités offertes par le workflow standard d'un traitement ?.*

Demander une description du traitement à son propriétaire

Pour adresser le traitement à son propriétaire :

- Faites un clic droit sur le traitement et sélectionnez :



Le propriétaire de traitement peut se connecter à **HOPEX Privacy Management** avec le profil correspondant et compléter la description du traitement.

☛ *Vous devez avoir au préalable sélectionné un propriétaire de traitement dans la page de propriété du traitement.*

Soumettre la description du traitement

Après avoir décrit le traitement, le propriétaire peut l'adresser aux membres de l'équipe Privacy.

L'équipe Privacy peut lancer une évaluation préliminaire sur la base des informations spécifiées par le propriétaire du traitement.

Soumettre évaluations préliminaires et DPIA

Après que le propriétaire du traitement a complété et soumis la description, le responsable de la confidentialité peut évaluer le traitement (évaluations préliminaires et DPIA le cas échéant).

☛ *Si la description du traitement se révèle insuffisante, un membre de l'équipe Privacy peut décider de la renvoyer au propriétaire du traitement pour qu'il la modifie.*

RAPPORTS ASSOCIÉS AUX TRAITEMENTS

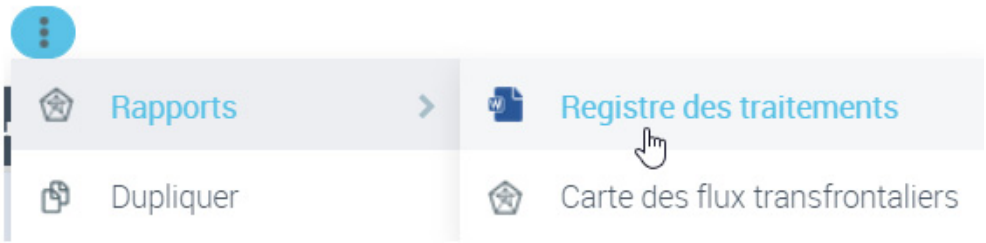
Accéder aux rapports associés aux traitements

Pour générer des rapports sur des traitements :

1. Sélectionnez un traitement.

   ☛ *Voir Accéder aux traitements.*

2. Sélectionnez un des rapports disponibles via le menu déroulant **... > Rapports**.



Registres des traitements

☛ *Voir Accéder aux rapports associés aux traitements.*

A propos du registre des traitements

Les informations collectées dans le registre des traitements sont au cœur du système de documentation de protection des données. Elles doivent être disponibles à tout moment en cas de demande de l'autorité de protection des données.

> 🕮 *Une autorité chargée de la protection des données est une autorité nationale dont la tâche est d'assurer la protection et la confidentialité des données, ainsi que de surveiller et de faire appliquer les réglementations concernant la protection des données au sein de l'Union Européenne.*

Le registre des traitements indique ***qui*** traite ***quelles*** données personnelles, ***où***, ***pourquoi***, et ***comment***.

Créer un registre des traitements

Pour générer un registre des traitements sous la forme d'un document Word :

1. Dans le menu de navigation, cliquez sur **Traitements**.
2. Sélectionnez un traitement et dans le menu déroulant associé au bouton **Rapports**, sélectionnez **Registre des traitements**.

Un document Word est généré. Il contient le contenu suivant :

- ***Introduction***: elle décrit les droits des personnes concernées, le principe des transferts de données et des mesures de sécurité.
- ***Liste des Traitements***
- ***Description détaillée des traitements sélectionnés***
  - Rôle de protection de données
    - ☛ *Voir Vue globale des traitements.*
  - Activités sensibles
    - ☛ *Voir Vue globale des traitements.*
  - Fondement juridique
    - ☛ *Voir Fondement juridique du traitement.*
  - Catégories de données et catégories de personnes concernées
    - ☛ *Voir Vue globale des traitements.*
  - Gestion des informations et du consentement
    - ☛ *Voir Gestion des droits des personnes concernées et des informations.*
  - Droits des personnes concernées
    - ☛ *Voir Gestion des droits des personnes concernées et des informations.*
  - Transferts de données à des tierces parties
    - ☛ *Voir Transferts de données.*
  - Mesures de sécurité
    - ☛ *Voir Transferts de données.*
  - Éléments de sous-traitement
    - ☛ *Voir Vue globale des traitements.*
  - Pièces jointes
    - ☛ *Voir Accords contractuels et autres pièces jointes.*

Carte des flux transfrontaliers

Vous pouvez générer une carte des flux transfrontaliers qui affiche dans une carte mondiale les transferts de données sélectionnés.

☛ *Voir Accéder aux rapports associés aux traitements.*

Conditions préalables à l'utilisation d'une carte des flux transfrontaliers

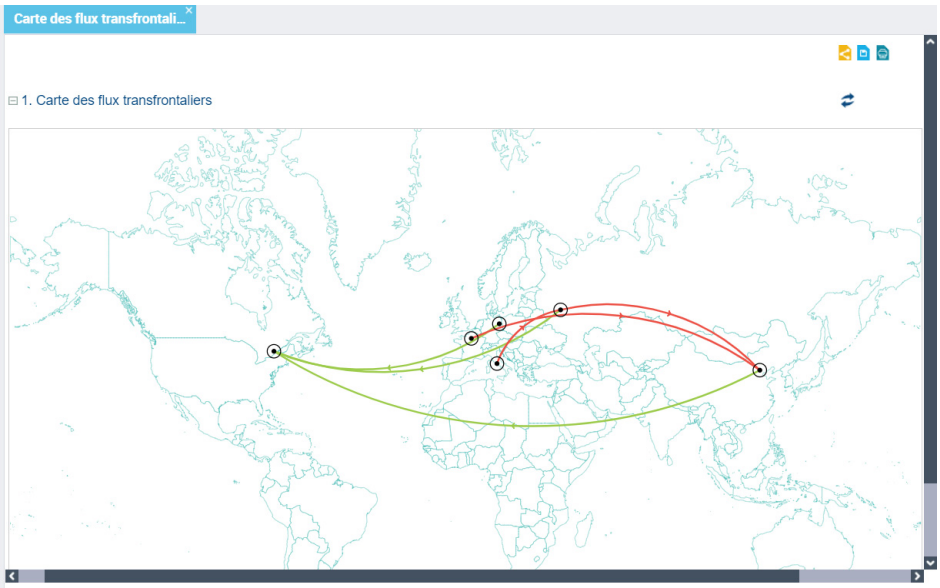
Assurez-vous que :

- un pays a été défini dans l'établissement siège des entités juridiques impliquées
  - ☛ *Pour plus de détails, voir Spécifier le pays d'une entité juridique.*
- vous avez défini à la fois le destinataire et l'émetteur du transfert
  - ☛ *Pour plus de détails, voir Spécifier les transferts de données sur un traitement.*

Contenu de la carte des transferts

Le pays du destinataire détermine si le transfert est adéquat ou non.

☛ *Dans le cas d'un transfert non adéquat vous pouvez rechercher l'établissement cible et les garanties qu'il applique. Pour plus de détails sur les garanties, voir Définir des garanties de transfert.*



☛ *Vous pouvez utiliser la molette de la souris pour effectuer un zoom avant ou arrière.*

Informations supplémentaires sur les transferts

Pour plus de détails sur la création de transferts, voir Spécifier les transferts de données sur un traitement.

Pour la résolution de problèmes, voir A propos des transferts.

Rapport spécifique à la CNIL

HOPEX Privacy Management vous permet de générer un rapport conforme aux exigences de la CNIL (Commission nationale de l'informatique et des libertés).

Activer le rapport CNIL

Ce fichier Excel qui porte sur les traitements est disponible en option dans le registre des traitements. Vous devez activer une option spécifique pour pouvoir générer ce rapport.

Pour activer le rapport CNIL :

1. Dans le menu principal, sélectionnez **Paramètres > Options**.
2. Dépliez le dossier **Privacy**.

3. Sélectionnez « Activer le rapport CNIL dans la liste du registre des traitements ».
4. Cliquez sur **OK**.

Conditions préalables au rapport CNIL

Pour les traitements à inclure dans le rapport, vous devez avoir spécifié le rôle de protection des données « Responsable de traitement » dans leur page de propriétés.

Générer le rapport CNIL

Pour générer ce rapport :

1. Dans le menu de navigation, sélectionnez **Traitements**.
2. Sélectionnez le traitement qui vous intéresse (sur lequel le rôle de protection des données « Responsable de traitement » a été spécifié).
3. A partir du bouton **Plus** de la barre d'outils, sélectionnez **Rapports > Registre de traitement - CNIL format**.

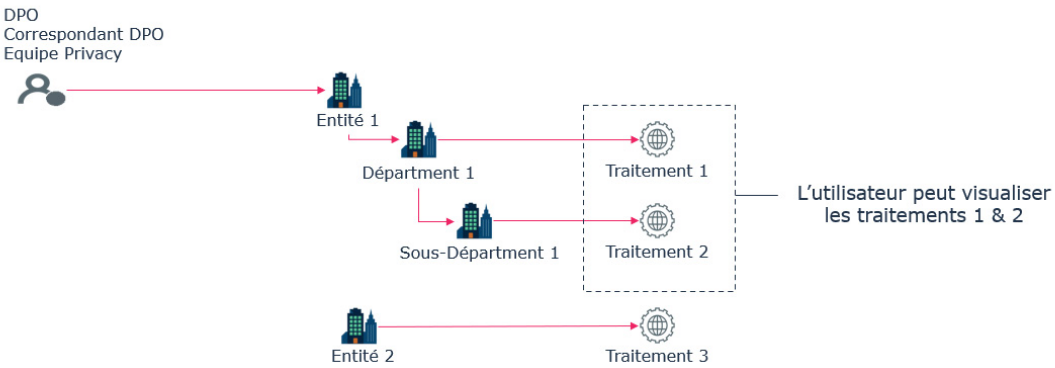
   ☛ *Si aucun traitement ne correspond au périmètre choisi, un avertissement apparaît.*
4. Spécifiez l'**Entité juridique** (responsable de traitement) qui exporte le registres de traitements.

   ☛ *Seules les entités juridiques reliées au registre de traitement qui ont pour rôle de protection des données « Responsable de traitement » sont proposées ici.*
5. Cliquez sur **OK**.

Le rapport Excel est généré.

GÉRER LA VISIBILITÉ DES TRAITEMENTS

Un utilisateur qui est affecté à une entité juridique ou à un département peut accéder aux traitements associés aux sous-entités juridiques ou sous-départements.

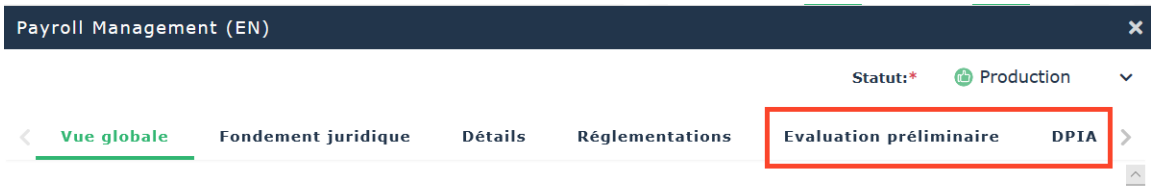


ÉVALUER LES TRAITEMENTS

L'équipe Privacy ou le DPO évaluent les traitements après description par le propriétaire de traitement.

☛ *Pour plus de détails sur la description des traitements, voir Gérer les traitements*

En tant que membre de l'équipe Privacy, vous êtes amené à utiliser les onglets suivants :



☛ *Pour des questions fréquentes concernant l'évaluation des traitements, voir A propos des évaluations.*

PRÉ-REQUIS À L'ÉVALUATION DES TRAITEMENTS

Pour pouvoir réaliser une évaluation (évaluation préliminaire ou DPIA), vous devez vous assurer que :

- les propriétaires de traitement ont décrit de manière appropriée les traitements.

  ☛ *Pour plus de détails, voir Gérer les traitements.*

- vous avez spécifié les niveaux de conformité sur la base des informations saisies par les propriétaires de traitement.

  ☛ *Voir Spécifier les niveaux de conformité.*

Spécifier les niveaux de conformité

L'équipe Privacy/le DPO doivent spécifier le niveau de conformité pour chaque section du traitement.

☛ *Il est nécessaire de donner des scores en fonction de ce que le propriétaire de traitement a renseigné sur le traitement. Ceci permettra de décider quels traitements doivent être évalués en premier (qu'il s'agisse d'évaluation préliminaire ou d'une DPIA).*

Niveau de conformité Fondement juridique

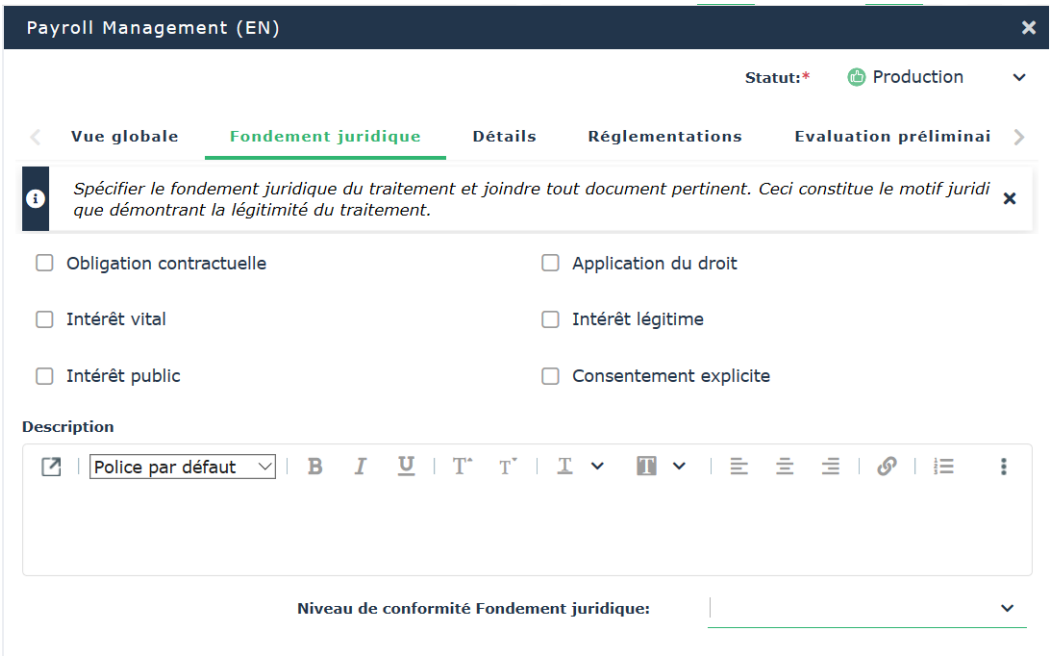
Pour spécifier un niveau de conformité concernant le fondement juridique :

1. Ouvrez la page de propriétés du traitement.

   ☛ *Voir Accéder aux traitements.*

2. Sélectionnez l'onglet **Fondement juridique**.

3. Sélectionnez une valeur dans le menu déroulant.



Au moins un fondement juridique doit être sélectionné. Si vous ne sélectionnez pas de fondement juridique pour le traitement, le traitement sera considéré comme étant peu conforme.

☛ *Pour plus de détails, voir Fondement juridique du traitement.*

Niveau de conformité Minimisation

Pour spécifier un niveau de conformité concernant la minimisation :

1. Ouvrez la page de propriétés du traitement.

   ☛ *Voir Accéder aux traitements.*
2. Sélectionnez l'onglet **Détails**.
3. Dépliez la section **Analyse de risque des données personnelles** de votre traitement.
4. Sélectionnez une valeur dans le menu déroulant.

   ☛ *Pour plus de détails sur la minimisation des données, voir Données à caractère personnel traitées.*

Transferts de données et mesures de sécurité

Pour spécifier un niveau de conformité concernant les transferts de données et les mesures de sécurité:

1. Ouvrez la page de propriétés du traitement.

   ☛ *Voir Accéder aux traitements.*
2. Sélectionnez l'onglet **Détails**.
3. Dépliez la section **Mesures de sécurité**.

4. Sélectionnez une valeur dans le menu déroulant.

   ☛ *Pour plus de détails, voir Transferts de données.*

Visualiser le niveau de conformité initial d'un traitement

Il est utile au DPO ou à l'équipe Privacy d'avoir une vision globale des niveaux de conformité du traitement. Cela permet de définir les priorités des actions ultérieures à mener (décider si vous avez besoin de réaliser une évaluation préliminaire ou une DPIA).

Pour identifier le niveau de conformité d'un traitement :

❱ Dans la page de propriété d'un traitement, sélectionnez l'onglet **Évaluation préliminaire**.

Ici vous trouvez un résumé des scores préalablement définis dans les onglets **Fondement juridique** et **Détails**.

- Fondement juridique (score défini dans l'onglet Fondement juridique)

  ☛ *Voir Fondement juridique du traitement.*

- Minimisation des données (score défini dans l'onglet Détails).

  ☛ *Voir Données à caractère personnel traitées.*

- Gestion des droits des personnes concernées et des informations (score défini dans l'onglet Détails)

  ☛ *Voir Gestion des droits des personnes concernées et des informations.*

- Transferts de données (score défini dans l'onglet Détails).

  ☛ *Voir Transferts de données.*

- Mesures de sécurité (score renseigné dans l'onglet Détails)

  ☛ *Voir Mesures de sécurité.*

RÉALISER UNE ÉVALUATION PRÉLIMINAIRE

L'objectif de l'évaluation préliminaire est d'identifier les traitements qui ont un faible niveau de conformité et qui nécessitent une DPIA ou des ajustements.

> ☛ *Nous vous recommandons, avant de réaliser l'évaluation préliminaire, de prendre connaissance des niveaux de conformité que le propriétaire de traitement a définis pour le traitement. Voir Visualiser le niveau de conformité initial d'un traitement.*

Consulter des rapports d'aide à la décision

Dans **HOPEX Privacy Management**, vous pouvez vous aider de votre tableau de bord pour identifier les priorités en termes de conformité et réaliser une évaluation préliminaire. Ceci vous permettra de vous focaliser sur les activités à risque dont le niveau de conformité dot être amélioré.

Votre tableau de bord contient par défaut différents graphiques sous forme de diagrammes en secteurs. Ils donnent une indication :

- sur le niveau de niveau de conformité final et l'échelle de risque après évaluation du traitement.

  > ☛ *Voir Traitements par niveau de conformité et Traitements par échelle de risque.*

- des traitements qui ont été évalués par l'intermédiaire d'une DPIA.

  > ☛ *Voir Traitements par statut d'évaluation (DPIA).*

  > ☛ *Veuillez noter que lorsque vous sélectionnez un secteur du digramme, les traitements correspondants s'affichent en bas du tableau de bord.*

Accéder à votre tableau de bord

Pour accéder à votre tableau de bord :

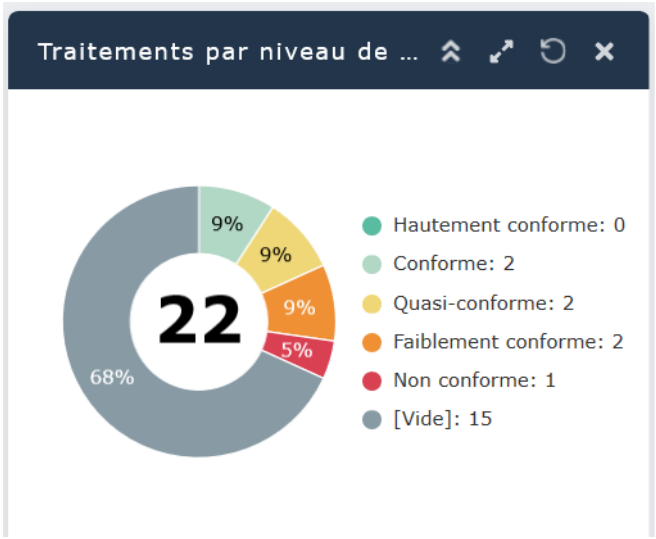
1. Dans le menu de navigation, cliquez sur **Tableau de bord**.

   > ☛ *Les rapports de votre tableau de bord prennent en compte tous les objets que vous êtes autorisé à visualiser.*

Traitements par niveau de conformité

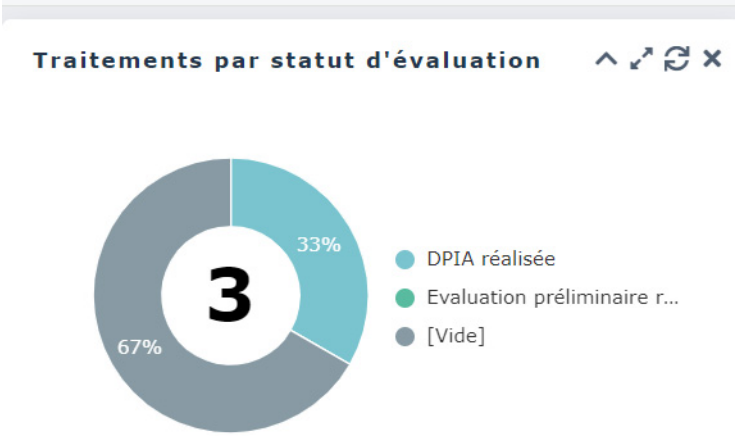
Le diagramme en secteurs vous permet de visualiser les traitements qui sont conformes au RGPD.

> ☛ *Les informations affichées proviennent des évaluations préliminaires ou des DPIA (le résultat du plus récent des deux types d'évaluation est pris en compte).*



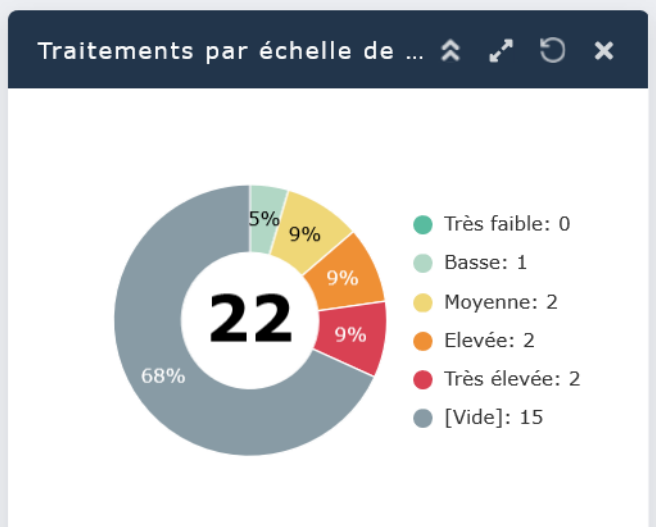
Traitements par statut d'évaluation (DPIA)

Ce diagramme en secteurs illustre le nombre de traitements qui ont été évalués ***via une DPIA***. Vous devez vous concentrer sur les traitements qui n'ont pas encore fait l'objet d'une DPIA.



Traitements par échelle de risque

Le diagramme en secteurs affiche les traitements qui sont considérés à risque.



☛ *Les informations affichées proviennent des évaluations préliminaires ou des DPIA (le résultat du plus récent des deux types d'évaluation est pris en compte).*

Réaliser une évaluation préliminaire

En vous basant sur les scores de conformité proposés par le tableau de bord de l'évaluation préliminaire, vous pouvez :

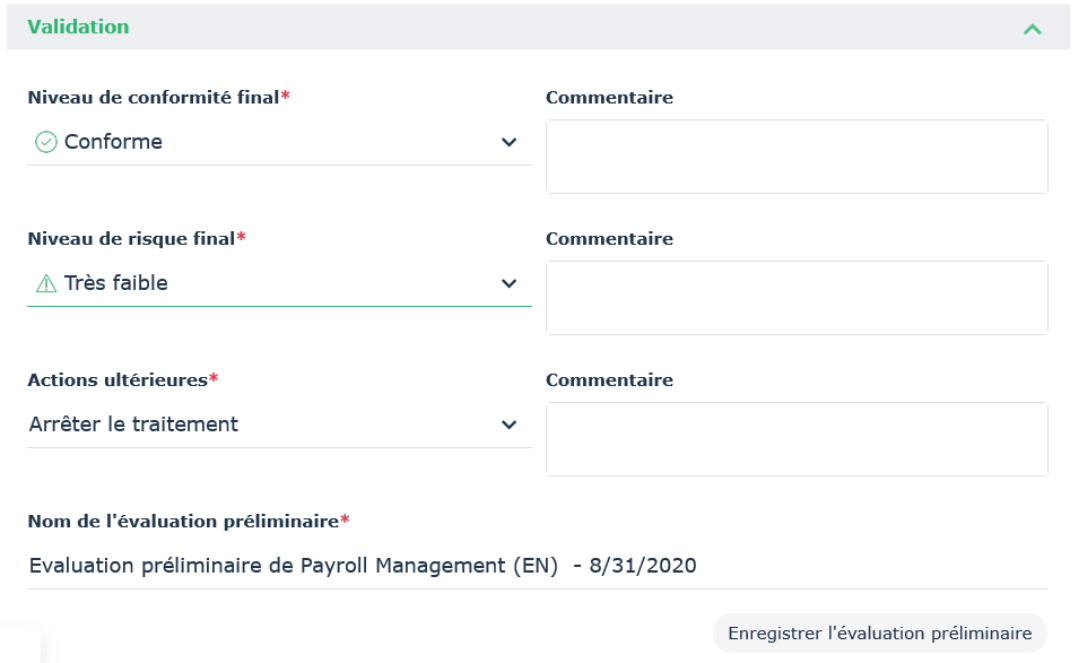
- Donner un score de validation final
- Définir les actions ultérieures

Pour enregistrer votre évaluation préliminaire :

1. Dans l'onglet **Évaluation préliminaire** de la page de propriété du traitement, dépliez la section **Validation**.
2. Sélectionnez une valeur pour le **Niveau de conformité final** et pour le **Niveau de risque final**.

   ☛ *Ces champs sont initialisés à partir des différents niveaux de conformité qui ont été saisis préalablement. Pour plus de détail sur les calculs permettant d'obtenir les valeurs proposées par défaut, voir la section Questions Fréquentes, "A propos des évaluations".*
3. Saisissez un commentaire pour justifier votre choix.
4. Indiquez les **Actions ultérieures** à réaliser :
   - Rien
   - Arrêter le traitement
   - Notifier l'autorité de contrôle
   - Autres

5. Une fois que vous avez saisi toutes les informations nécessaires, cliquez sur **Enregistrer l'évaluation préliminaire**.



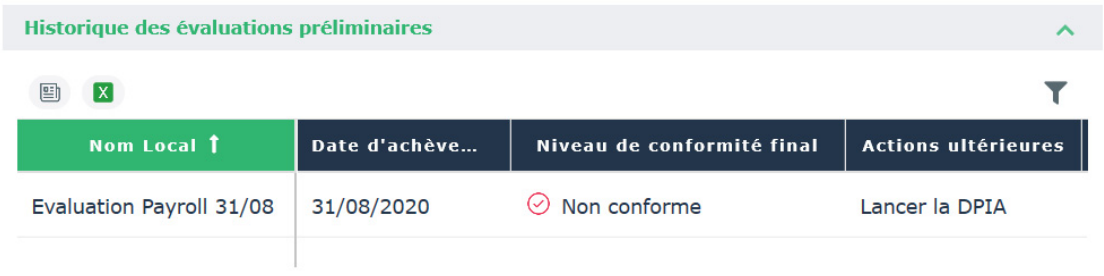
☛ *Si le niveau de conformité final est faible, vous devez réaliser une DPIA. Pour plus de détails, voir Réaliser une analyse d'impact (DPIA).*

Consulter l'historique des évaluations préliminaires

Lorsque vous enregistrez l'évaluation préliminaire, celle-ci est stockée dans la section **Historique** avec les valeurs que vous avez saisies.

Pour accéder à l'historique des évaluations préliminaires :

- Dans l'onglet **Évaluation préliminaire** de la page de propriété du traitement, dépliez la section **Historique des évaluations préliminaires**.



Vous pouvez consulter les pages de propriétés de l'évaluation préliminaire en mode lecture seule.

RÉALISER UNE ANALYSE D'IMPACT (DPIA)

A propos des DPIA

Quand réaliser une DPIA ?

Si l'évaluation préliminaire indique un risque élevé, vous (en tant que DPO ou membre de l'équipe Privacy) devez réaliser une DPIA.

> ☛ *Pour plus de détails sur les évaluations préliminaires, voir Réaliser une évaluation préliminaire.*

Lorsque le traitement est susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées, il est obligatoire de réaliser une DPIA.

Qu'est-ce qu'une DPIA ?

Une DPIA est une évaluation de risque détaillée.

La DPIA doit afficher :

- Les caractéristiques du traitement
- Les risques qui peuvent avoir un impact sur la conformité.

  > ☛ *Pour plus de détails, voir Créer et évaluer des risques pour une DPIA.*

- Les actions correctives qui permettent d'assurer que le traitement est sous contrôle.

  > ☛ *Pour plus de détails, voir Recommandations et mesures correctives de DPIA.*

Créer une DPIA

Créer une DPIA

Pour démarrer une nouvelle DPIA:

1. Dans la page de propriétés du traitement, sélectionnez l'onglet **DPIA**.
2. Cliquez sur **Démarrer la DPIA**.
   Dans la fenêtre qui apparaît, les niveaux de risques identifiés lors de votre évaluation préliminaire apparaissent.

Il se peut que vous préfériez ouvrir une DPIA existante pour la modifier. Voir Réutiliser une DPIA.

Réutiliser une DPIA

Lorsqu'un traitement partage les mêmes risques qu'un autre traitement, vous pouvez réutiliser une DPIA existante.

Pour ce faire, vous devez importer une DPIA, ce qui consiste à importer les risques et les recommandations associés. De cette façon vous pouvez bénéficier de ce que vous avez réalisé dans une précédente DPIA. Vous pouvez la modifier pour l'adapter au traitement qui vous intéresse.

Pour importer une DPIA :

1. Voir Accéder aux traitements.
2. Dans la page de propriété du traitement, sélectionnez l'onglet **DPIA**.
3. Cliquez sur **Démarrer la DPIA**.
4. Dans la page de création d'une DPIA, cliquez sur **Importer une DPIA**.
5. Sélectionnez une DPIA existante.

   ☛ *La DPIA concernée doit déjà exister dans l'historique des DPIA.*

Les données saisies dans la DPIA sélectionnée sont importées. Vous pouvez ensuite les modifier pour les adapter à votre DPIA en cours.

Modifier une DPIA

Lorsqu'une DPIA existe déjà et s qu'elle n'a pas été finalisée, vous pouvez la modifier via le bouton **Modifier la DPIA**.

☛ *Lorsque la DPIA a été finalisée, le bouton **Modifier la DPIA** n'est plus disponible. Vous devez alors démarrer une nouvelle DPIA. Pour plus de détails, voir Créer une DPIA.*

Créer et évaluer des risques pour une DPIA

Vous venez de créer une DPIA.

☛ *Pour plus de détails, voir Créer une DPIA.*

La première étape lors de la réalisation d'une DPIA consiste à définir et évaluer les risques.

Pour créer des risques dans une DPIA :

1. Dans la section **Risques pour le respect de la vie privée** de la DPIA, cliquez **Nouveau** pour créer un risque dans l'un des onglets correspondants aux différents types de risque:
   - **Accès illégitime**
   - **Perte de données**
   - **Intégrité des données**
   - **Non disponibilité des données**
   - **Traitement illicite**

2. Dans la première page de l'assistant, saisissez les informations suivantes:
   - **Nom du risque**
   - **Impact sur les personnes concernées** : causes les plus courantes qui peuvent engendrer ce risque.
   - **Impact sur les personnes concernées**: impacts sur les personnes concernées si le risque se matérialise.
   - **Description du risque**

> ☛ *Si des risques ont déjà été créés lors de la réalisation d'une DPIA sur d'autres traitements, cette page vous propose de **Réutiliser un risque existant**.*

3. Cliquez sur **Suivant**.
4. Dans la seconde page de l'assistant, procédez à l'évaluation du risque :
   - **Sévérité du risque** : de « Très faible » ou « Elevée »
   - **Probabilité** : de « Rare » à « Certaine »

5. (optionnel) Sélectionnez un groupe de **Mesures de sécurité** prises pour traiter ce risque.

   ☛ *Les mesures de sécurité sont des données de référence définies par le responsable de la confidentialité. Pour plus de détails, voir Définir les mesures de sécurité.*

   - *Technique*
   - *Organisationnel*
   - *Certification*

   ☛ *Pour plus d'informations sur ces mesures de sécurité, voir Spécifier des mesures de sécurité sur un traitement.*

6. Cliquez sur **OK**.

Recommandations et mesures correctives de DPIA

Lorsque vous réalisez une DPIA, vous pouvez définir :

- Des recommandations d'ordre général
- Des actions correctives se basant sur des plans d'action

Créer des recommandations

Les recommandations sont basées sur les évaluations de risque préalablement créées dans le cadre de la DPIA.

☛ *Pour plus de détails, voir :*

- *Créer une DPIA*
- *Créer et évaluer des risques pour une DPIA*

Pour créer des recommandations dans le cadre d'une DPIA :

1. Dans l'assistant de création de la DPIA, dépliez la section **Recommandations et actions correctives**.
2. Dans le champ **Description du risque**, sélectionnez une ou plusieurs évaluations de risque pour les relier à la recommandation en cours de création.

Vous pouvez également spécifier les informations suivantes sur votre recommandation :

- **Description de la recommandation** : saisir un commentaire pour décrire la recommandation
- **Risque cible**: spécifier le risque visé obtenu suite aux mesures correctives mises en œuvre.

Définir des mesures correctives

Après avoir émis des recommandations d'ordre général, vous pouvez décider de mettre en place de véritables plans d'action. Cela vous permettra de suivre les actions mises en œuvre pour atténuer les risques.

☛ *Un plan d'action comprend une série d'actions, son objectif étant de réduire les risques et événements ayant un impact négatif sur les activités de l'entreprise.*

Pour plus de détails, voir Gérer les plans d'action.

Valider la DPIA

Une fois que vous créé la DPIA ainsi que des risques, vous pouvez valider la DPIA.

> ☛ *Pour plus de détails, voir :*
>
> - *Créer une DPIA*
> - *Créer et évaluer des risques pour une DPIA*

Pour valider une DPIA :

1. Dans l'assistant de création de la DPIA, dépliez la section **Validation**.
2. Spécifiez les informations suivantes pour tirer les conclusions de la DPIA.

Niveau de risque final

- Très faible
- Faible
- Moyen
- Élevé
- Très élevé

Niveau de conformité final

- Non conforme
- Faiblement conforme
- Quasi-conforme
- Conforme

> ☛ *Ce champ est initialisé à partir des différents niveaux de conformité qui ont été saisis préalablement.*

Action ultérieure

Dans cette section vous devez spécifier l'action à suivre en vous basant sur les différents indicateurs obtenus :

- Rien
- Arrêter le traitement
- Notifier l'autorité de contrôle

Consulter les rapports et les résultats de la DPIA

Visualiser le tableau de bord du traitement

Après avoir réalisé la DPIA, le tableau de bord de l'onglet **Vue globale** de la page du traitement affiche des données qui prennent en compte les résultats de la DPIA.

Niveau de conformité global et dernières échelles de risque

Ces indicateurs sont calculés sur la base des dernières évaluations préliminaires ou de la DPIA.

☛ *L'évaluation la plus récente est prise en compte.*

Dernière évaluation

Cet indicateur permet de savoir quand la dernière évaluation a été réalisée (qu'il s'agisse d'une évaluation préliminaire ou d'une DPIA).

Registre des DPIA

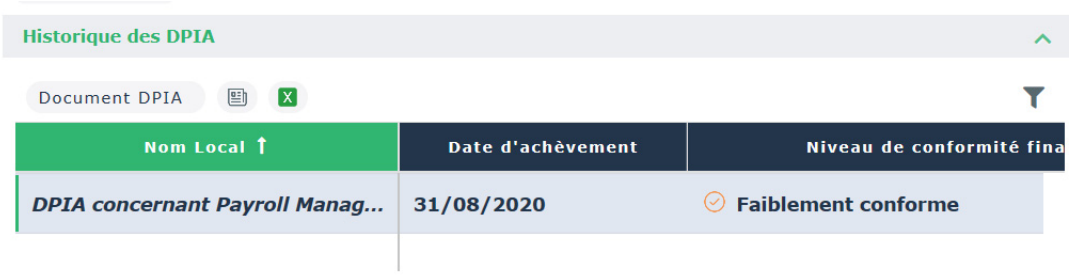
Voir Registre des DPIA.

Générer un document de DPIA

Pour générer un document relatif à une DIPA :

1. Dans l'onglet **DPIA** de la page de propriété d'un traitement, dépliez l'onglet **Historique des DPIA**.

2. Sélectionnez une DPIA et cliquez sur **Document DPIA**.



Le résumé de la DPIA contient les informations suivantes :

- Le niveau de conformité global du traitement défini préalablement à la DPIA.
- Un récapitulatif des différents risques identifiés au cours de la DPIA, avec leur impact et les recommandations destinées à atténuer ces risques.
- Le niveau de risque final et le niveau de conformité final obtenus après avoir réalisé l'évaluation de risque.

GÉRER LES VIOLATIONS DE DONNÉES

HOPEX Privacy Management permet au responsable de traitement de conserver un registre des violations des données, comme la loi l'impose.

HOPEX Privacy Management permet également de définir les éléments suivants :

- évaluer la gravité du point de vue de la personne concernée
- à partir de l'évaluation de la gravité, décider qui doit être notifié de la violation
  - dans le cas d'un risque associé à la violation, l'autorité de contrôle doit en être informée
  - lorsque le risque est élevé, la personne concernée doit en être informée
- identifier les mesures correctives sous forme de plans d'action

☛ *Ces actions peuvent être suivies par les autres solutions **HOPEX**.*

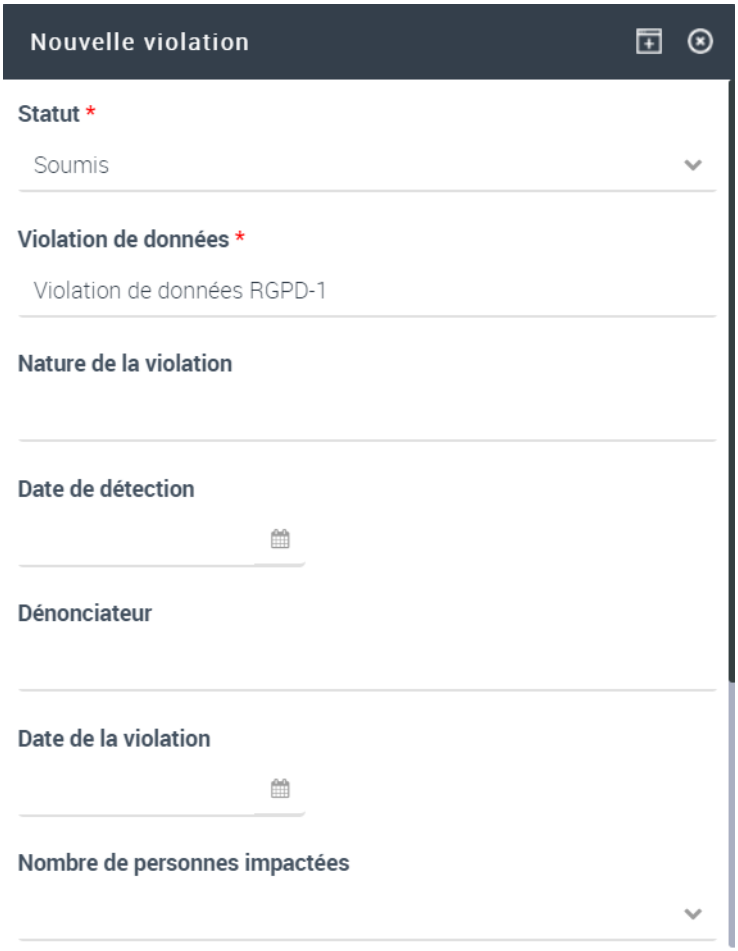
Déclarer une violation de données

Toute personne peut saisir une violation de données dans **HOPEX Privacy Management**.

Exemple de violation de données : Un employé accède aux données auxquelles il n'est pas autorisé à accéder.

Pour saisir une violation de données :

1. Dans le menu de navigation sélectionnez **Violations** et cliquez sur **Nouveau**.



2. Décrivez la violation de données :
   - **Date de détection**

     ☛ *La date de détection est importante puisque vous avez 72 heures pour collecter, évaluer et signaler la violation. Voir Voir le temps écoulé depuis la détection de la violation.*
   - **Dénonciateur** : partie prenante qui signale l'incident
   - **Date de la violation**
   - **Nombre de personnes impactées**
   - **Source** : réclamation externe, contrôle interne, alerte interne, autre
   - **Catégories de données impliquées**

     ☛ *Pour plus de détails, voir Définir les catégories de données.*
   - **Personnes concernées impactées**

     ☛ *Pour plus de détails, voir Définir les catégories de personne concernée.*

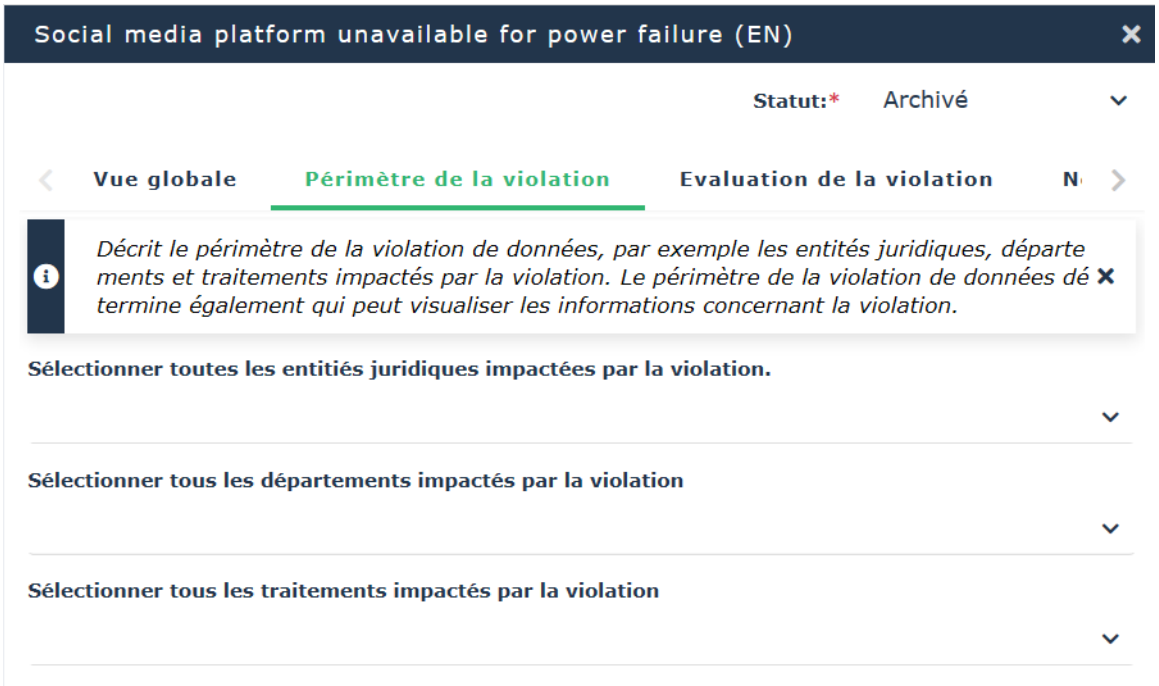
Une fois la violation créée, vous pouvez fournir des informations sur :

- Le périmètre de la violation
- l'évaluation de la violation : voir Évaluer une violation de données
- la notification de la violation : voir Notifier une violation de données

Définir le périmètre de la violation de données

Vous pouvez décrire le périmètre de la violation de données, autrement dit les entités juridiques, les départements et les traitements qui sont touchés par la violation de données.

Le périmètre de la violation de données détermine également qui peut voir les informations de la violation.



Évaluer une violation de données

Pour évaluer une violation de données :

1. Dans le menu de navigation, cliquez sur **Violations**.
2. Sélectionnez une violation de données et dans sa page de propriétés, sélectionnez l'onglet **Évaluation de la violation**.

Ici vous pouvez :

- décrire les conséquences de la violation
- créer des mesures correctives
- désigner une personne responsable de la gestion et du suivi de la violation de données

☛ *Pour plus de détails, voir Planifier des mesures correctives.*

Planifier des mesures correctives

Vous devez prendre des mesures appropriées afin d'empêcher les violations de données.

Pour créer des mesures correctives :

1. Dans le menu de navigation, cliquez sur **Violations**.
2. Sélectionnez une violation de données et dans sa page de propriétés, sélectionnez l'onglet **Évaluation de la violation**.
3. Sous **Mesures correctives**, cliquez sur **Nouveau**.
4. Saisissez un commentaire pour décrire comment remédier à la violation de données.
5. Spécifiez le statut de la mesure corrective :
   - Mis en œuvre
   - En cours
   - Prévu

   ☛ *Vous pouvez modifier le statut par la suite.*
6. Cliquez sur **OK**.

Notifier une violation de données

Lorsqu'une violation de données est constatée, il peut être nécessaire d'informer les autorités de contrôle ou les personnes concernées. Dans ce cas il convient de détailler la façon dont est gérée la notification.

Pour décrire une notification de violation de données :

1. Dans le menu de navigation, cliquez sur **Violations**.
2. Sélectionnez une violation de données et dans sa page de propriétés, sélectionnez l'onglet **Notification de la violation**.

Vous pouvez indiquer si la violation de données exige :

- **de notifier les personnes concernées**

  ☛ *Saisissez une **Date de notification des personnes concernées**.*
- **de notifier l'autorité de contrôle**

  ☛ *Spécifiez :*
  - ***Les autorités de contrôles notifiées***
  - ***La date de notification auprès des autorités***

Voir le temps écoulé depuis la détection de la violation

Suite à la détection d'une violation, vous disposez d'un certain nombre d'heures pour agir et faire le signalement aux autorités ou personnes concernées.

HOPEX Privacy Management calcule automatiquement cette information pour vous.

Pour voir le nombre d'heures écoulées depuis la détection de la violation :

1. Dans le menu de navigation, cliquez sur **Violations**.
2. Dans la liste des violations, sélectionnez celle qui vous intéresse et consultez la colonne **Temps écoulé (heures) depuis la découverte de la violation**.

Dupliquer des violations de données

Vous pouvez dupliquer des violations de données.

Pour ce faire :

1. Dans le menu de navigation, cliquez sur **Violations**.
2. Dans la liste des violations, sélectionnez celle qui vous intéresse et cliquez sur **Dupliquer**.
3. Dans l'assistant qui apparaît, sélectionnez les sections à dupliquer et cliquez sur **OK**.

Documenter la violation de données

Pour décrire précisément la violation de données :

1. Dans le menu de navigation, cliquez sur **Violations**.
2. Dans la fenêtre de propriétés d'une violation, sélectionnez la page **Pièces jointes**.
3. Déposez ou ajouter un document.

GÉRER LES DEMANDES DES PERSONNES CONCERNÉES

Les lois de protection des données octroient aux personnes concernées des droits spécifiques sur leurs données personnelles. Ces droits incluent l'obtention de copies des données personnelles, les demandes de changements de ces dernières, la restriction de leur traitement, leur suppression ou leur réception dans un format électronique afin de les transférer à un autre responsable de traitement.

📖 Une demande de personne concernée est une demande formelle adressée à un responsable de traitement pour qu'il intervienne sur ses données à caractère personnel.

La législation exige de que le responsable de traitement conserve toutes les demandes qui émanent des personnes concernées. **HOPEX Privacy Management** vous permet de répondre à cette exigence et d'assurer le suivi de ces demandes dans les meilleurs délais.

Créer une demande de personne concernée

Vous devez enregistrer les demandes de personnes concernées que vous avez reçues.

Pour créer une demande de personne concernée :

1. Dans le menu de navigation, cliquez sur **Personnes concernées > Demandes des personnes concernées**.
2. Cliquez sur **Nouveau**.

Vous pouvez fournir les informations suivantes :

- **Statut de la demande**
  - Demande en attente
  - Nouvelle
  - Assignée
  - En cours de traitement
  - Fermée
- **Type de demande**
  - Accès

    📖 *Le droit d'accès permet aux personnes concernées d'accéder aux données à caractère personnel les concernant et que le responsable de traitement détient.*
  - Effacement

    📖 *Une personne concernée peut avoir le droit de demander à supprimer des données la concernant que vous avez en votre possession.*
  - Opposition

    ☛ *La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant.*
  - Droit à l'oubli

    📖 *Le droit à l'oubli est également appelé Droit à l'effacement. Il autorise la personne concernée à faire supprimer ses données à caractère personnel par le responsable de traitement, à stopper la dissémination de ses données, et à interdire leur traitement par des tiers.*
  - Rectification

    ☛ *Toute personne concernée devrait pouvoir obtenir du responsable de traitement et dans les meilleurs délais la rectification des données à caractère personnel inexactes la concernant.*
  - Portabilité

    📖 *La portabilité est l'exigence pour les responsables de traitement de fournir à toute personne concernée une copie de ses données dans un format permettant à un autre responsable de traitement d'en faire usage.*
  - Limitation

    ☛ *La personne concernée devrait avoir le droit d'obtenir du responsable du traitement la limitation du traitement.*
- **Date de la demande**

  ☛ Il est obligatoire de spécifier la date de la demande. Cette date permettra de calculer automatiquement le nombre de jours qui se sont écoulés depuis la demande émanant de la personne concernée.
- **Nom de la personne concernée**

Détailler la demande de personne concernée

Pour décrire plus en détail la demande d'une personne concernée, vous pouvez ajouter les informations suivantes :

- **Origine de la demande**
  L'origine de la demande est le moyen par lequel la demande est envoyée.

  `Par exemple : l'identifiant d'un formulaire sur le web`
- **Type de document**
  Il est important d'enregistrer un document officiel pour identifier de manière claire la personne concernée. Ce document peut être :
  - Une carte d'identité
  - Un passeport
  - Un permis de conduire
  - Autres
- **Numéro du document** : correspond au numéro du document référencé ci-dessus
- **Demande en provenance de la personne concernée**

  ☛ Vous pouvez saisir un commentaire dans ce cadre.
- **Priorité de la demande**
  - Élevée
  - Moyenne
  - Basse
- **Personne assignée**
- **Tag**

  ☛ *Vous pouvez sélectionner des tags de façon à faciliter la recherche plein texte. Pour plus de détails sur les tags, voir "Fonctionnalités collaboratives".*

Décrire le périmètre de la demande de la personne concernée

Il est nécessaire de décrire le périmètre de la demande émanant de la personne concernée, par exemple quelles entités et quels départements sont impactés par la demande. Vous pouvez également donner plus de détails et associer un traitement.

Pour décrire le périmètre de la demande de la personne concernée :

1. Dans le menu de navigation, cliquez sur **Personnes concernées > Demandes des personnes concernées**.
2. Dans la page de propriétés de la demande de la personne concernée, sélectionnez l'onglet **Périmètre de la demande**.
3. A partir des listes déroulantes, sélectionnez les éléments impactés :
   - entités juridiques
   - départements
   - et/ou traitements

   ☛ Veuillez noter que le nombre de demandes de personnes concernées est un critère important qui peut constituer un Indicateur Clé de Performance.

Joindre des documents à la demande

Il peut être utile de fournir des documents pour décrire de manière détaillée la demande émanant de la personne concernée (par exemple l'email reçu).

Pour joindre un document à la demande :

1. Dans le menu de navigation, cliquez sur **Personnes concernées > Demandes des personnes concernées**.
2. Dans la page de propriétés de la demande, sélectionnez l'onglet **Pièces jointes**.
3. Créer une pièce jointe et spécifiez :
   - l'ID du document
   - le titre du document
   - la description du document
4. Dans **Emplacement du fichier**, sélectionnez le document à joindre.
5. Cliquez sur **Upload** puis sur OK.

Gérer les échéances des demandes

Le nombre de jours qui se sont écoulés depuis la demande émanant d'une personne concernée est automatiquement calculé.

Lorsque la date limite des 30 jours approche, et si la demande n'est pas « fermée », la personne responsable de la gestion de la demande est notifiée par email.

Au bout de 30 jours, vous pouvez indiquer que vous souhaitez prolonger la date d'échéance, comme le prévoit la législation.

Pour repousser l'échéance de la demande émanant d'une personne concernée :

1. Dans le menu de navigation, cliquez sur **Personnes concernées > Demandes des personnes concernées**.
2. Dans les colonnes disponibles sur la demande, cochez la case **Prolongation de la date limite**.

GÉRER LES PLANS D'ACTION

La fonctionnalité de gestion des plans d'action consiste à définir, exécuter et suivre un certain nombre d'actions.

> 🕮 *Un plan d'action comprend une série d'actions, son objectif étant de réduire les risques et événements ayant un impact négatif sur les activités de l'entreprise.*

ACCÉDER AUX PLANS D'ACTION

Accéder à tous les plans d'action

Pour accéder aux plans d'action dans **HOPEX Privacy Management** :

- Dans le menu de navigation, cliquez sur **Plans d'action**.

Vous trouvez ici une liste de plans d'action classée en fonction de différents critères :

- Tous les plans d 'action
  - ☛ *Affiche tous les plans d 'action*
- Plans d'action en retard
  - ☛ *Affiche les plans d'action dont la date de fin planifiée est dépassée*
- Mes plans d'action
  - ☛ *Affiche les plans d'action dont vous êtes propriétaire*
- Mes plans d'action en retard
  - ☛ *Affiche les plans d'action dont vous êtes propriétaire et dont la date de fin planifiée est dépassée*

Accéder aux plans d'action spécifiques à un traitement

Pour accéder aux plans d'action spécifiques à un traitement :

1. Dans le menu de navigation, sélectionnez **Traitements**.
2. Ouvrez la page de propriétés d'un traitement et sélectionnez l'onglet **Plans d'action**.

DÉFINIR LES PLANS D'ACTION

Pour définir un plan d'action :

1. Voir Accéder aux plans d'action.
2. Ouvrez la fenêtre de propriétés du plan d'action qui vous intéresse.
   Dans la page **Caractéristiques**, les sections suivantes apparaissent :

Caractéristiques générales

Dans la section **Caractéristiques**, vous pouvez spécifier des champs sur le plan d'action, par exemple :

- **Nom** : nom du plan d'action
- **Propriétaire** : est par défaut l'utilisateur qui a créé le plan d'action.
- **Tags**
- **Entité propriétaire** : permet de restreindre la liste des propriétaires.
- Approbateur : utilisateur chargé de valider le plan d'action lorsque toutes les actions sont terminées.
- **Moyens** : description textuelle des moyens requis/souhaités pour l'exécution du plan d'action.
- **Priorité** : permet de spécifier un degré de priorité La priorité peut être :
  - Faible
  - Moyenne
  - Élevée
  - Critique
- **Origine** : permet de définir le contexte de mise en œuvre du plan d'action
  - Audit
  - Conformité
  - Événement
  - Risque, Demande de changement
  - Autres
- **Catégorie** : permet de spécifier l'action entreprise, par exemple : Amélioration des processus
- **Nature** : permet de définir le plan d'action mis en œuvre :
  - Préventif
  - Correctif
- **Description** : donne des informations supplémentaires sur le plan d'action et ses caractéristiques.

Analyse Financière

- **Coût prévu** : estimation du coût du plan d'action, exprimé dans la **Devise**.
- **Coût réel** : coût réel du plan d'action, exprimé dans la **Devise**.
- **Coût prévu (Jours-homme)** : estimation en jours.homme de la charge de travail liée à la mise en œuvre du plan d'action.
- **Coût réel (Jours-homme)** : coût lié à la mise en œuvre du plan d'action, exprimé en jours.homme.

Facteurs de succès et résultat

Dans la section **Facteurs de succès et résultat**, vous pouvez saisir les indicateurs de succès permettant d'évaluer la réussite du plan d'action.

- **Facteur clé de succès** : information textuelle concernant les facteurs principaux qui ont contribué à la réussite du plan d'action.
- **Résultat** : permet d'indiquer si le plan d'action a réussi ou échoué.
  - Non connu
  - Echec
  - Succès
- **Commentaires concernant le résultat** : information textuelle concernant les résultats du plan d'action.

Périmètre

Dans **HOPEX Privacy Management**, vous devez positionner le plan d'action sur un traitement.

Jalons

Les jalons sont des dates importantes. Vous pouvez les spécifier plus tard.

- **Date de début planifiée** et **Date de début réelle**
- **Date de fin planifiée** et **Date de fin réelle**

Pièces jointes

Vous pouvez joindre des documents métier à un plan d'action :

☛ *Pour plus de détails sur l'utilisation des documents métier, voir le guide **HOPEX Common Features.***

GÉRER LES ACTIONS

Le propriétaire du plan d'action doit définir les actions permettant au plan d'action d'aboutir. Il a la possibilité de créer des actions et les affecter.

Pour créer un action à partir d'un plan d'action :

1. Voir Accéder aux plans d'action.
2. Ouvrez la fenêtre de propriétés du plan d'action.
3. Dans la section **Actions**, cliquez sur **Nouveau**.
4. Ouvrez la fenêtre de propriétés de l'action et spécifiez son **Nom**.
5. Saisissez les champs suivants :
   - **Propriétaire** : responsable de l'action comme spécifié par le créateur du plan d'action.
   - **Entité propriétaire** : permet de restreindre la liste des propriétaires de l'action.
6. Dans la section **Jalons**, spécifiez les dates importantes de l'action.
   - **Date de début planifiée** et **Date de début réelle**
   - **Date de fin planifiée** et **Date de fin réelle**

SUIVRE LES PLANS D'ACTION

L'avancement du plan d'action est renseigné par le responsable du plan d'action à des dates régulières. Pour plus de détails, voir Spécifier un taux d'avancement du plan d'action.

Pour envoyer automatiquement un rappel au responsable du plan d'action, vous pouvez relier un **Calendrier de pilotage** au plan d'action. Pour plus de détails, voir Utiliser les calendriers de pilotage.

Spécifier un taux d'avancement du plan d'action

Il est possible de spécifier un taux d'avancement du plan d'action si le statut du plan d'action est « en cours » (cela signifie qu'il a été validé).

Pour indiquer l'avancement d'un plan d'action :

1. Dans les propriétés du plan, dépliez la section **Historique de l'avancement**.
2. Dans la section **État d'avancement**, cliquez sur **Nouveau**.
   La page de création d'un **État d'avancement** apparaît.
3. Spécifiez le **Nom** de l'état d'avancement.
4. Spécifiez l'**Avancement (pourcentage)** et ajoutez un **Commentaire** si nécessaire.
5. Vérifiez la **Date d'avancement**
6. Saisissez une **Évaluation de l'avancement**.
   - Dans les temps
   - En retard

Utiliser les calendriers de pilotage

Vous pouvez relier un **Calendrier de pilotage** au plan d'action de manière à ce que le responsable du plan d'action puisse indiquer un pourcentage d'avancement à des dates définies dans le calendrier. Un message est alors envoyé automatiquement à l'utilisateur à ces dates.

> ☛ *Pour plus de détails sur la gestion des calendriers de pilotage, voir **HOPEX Customization (Windows) > Customizing Steering Calendars**.*

Pour relier un calendrier de pilotage à un plan d'action :

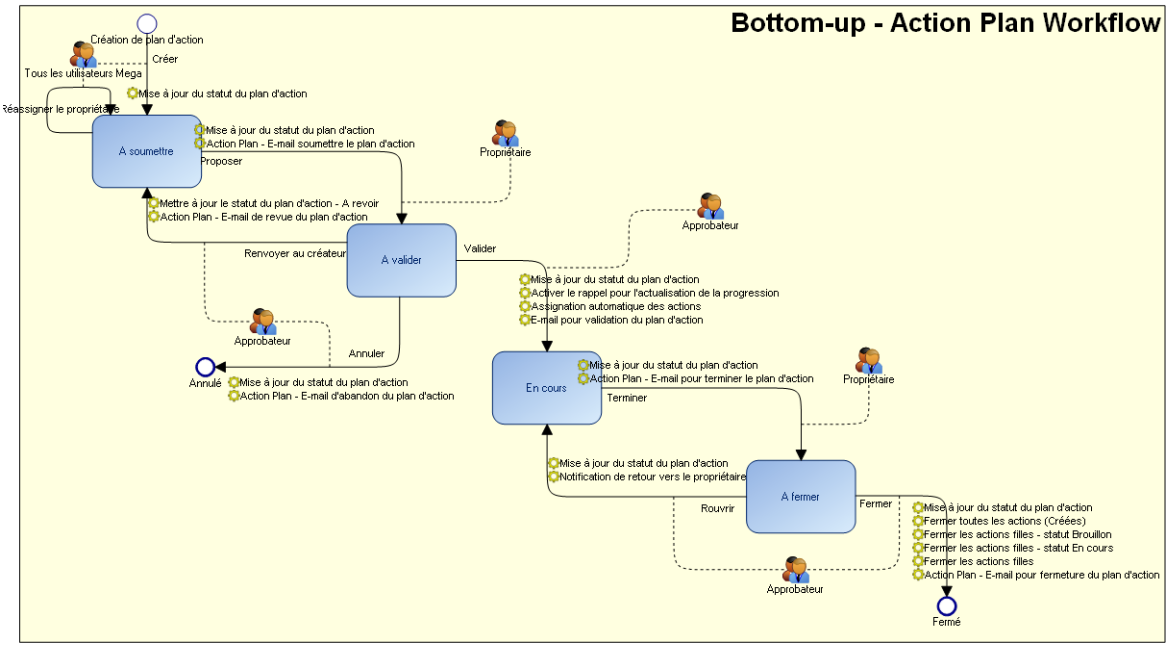
1. Ouvrez les propriétés du plan d'action.
2. Dans la section **Caractéristiques**, cliquez sur la flèche à droite du champ **Calendrier de pilotage**.
3. Sélectionnez un calendrier de pilotage (par défaut, "Plan d'action".

ANNEXE WORKFLOWS DE PLAN D'ACTION

Deux workflows sont proposés pour gérer les différentes étapes d'un plan d'action :

- Un workflow **Bottom-up**, qui correspond au cas dans lequel un plan d'action est créé par un utilisateur, par exemple un propriétaire de traitement. Ici le plan d'action créé doit être validé par un approbateur avant de pouvoir être mis en œuvre.
- Un workflow **Top-down**, qui correspond au cas dans lequel un plan d'action est créé par un gestionnaire de plan d'action, par exemple un DPO.

Workflow de plan d'action Bottom-up



Créer un plan d'action

Lorsqu'un propriétaire de traitement/d'application crée un plan d'action, le plan d'action se trouve dans l'état « A envoyer ».

Par défaut, le créateur du plan d'action est le **Propriétaire**. Après avoir spécifié les caractéristiques du plan d'action, le créateur peut :

- **Proposer** le plan d'action.
  Dans ce cas, l'utilisateur défini comme « Approbateur » reçoit un email, et le nouveau plan d'action apparaît avec le statut « A démarrer » dans sa liste de tâches.

Si vous avez modifié le nom de l'approbateur (qui est par défaut le créateur), vous devez **Ré-assigner** l'approbateur à partir du menu contextuel du plan d'action.

Préparer le plan d'action

L'approbateur peut :

- **Valider** après le passage du plan d'action en statut « En cours ». Des actions peuvent alors être créées. Pour plus de détails, voir Gérer les actions.
- **Annuler** le plan d'action, qui prend alors le statut « Annulé ».

Exécuter le plan d'action

Après avoir exécuté les actions du plan, le propriétaire peut :

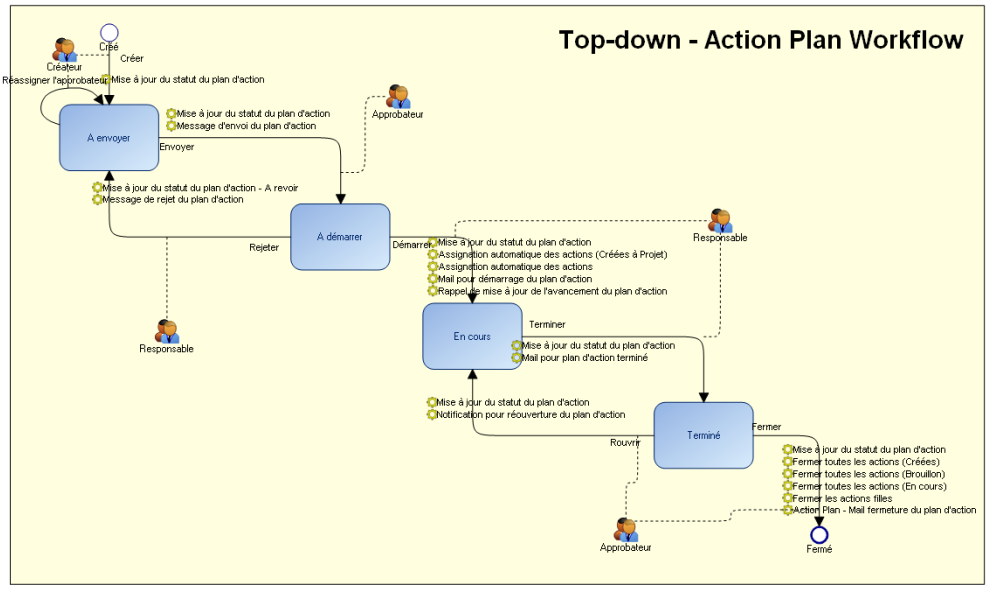
- **Terminer** le plan d'action, qui prend le statut « Fermé ». Pour ce faire, toutes les actions du plan d'action doivent être terminées. Pour plus de détails, voir Gérer les actions.
  L'approbateur est notifié de la demande de fermeture du plan d'action.

Fermer le plan d'action

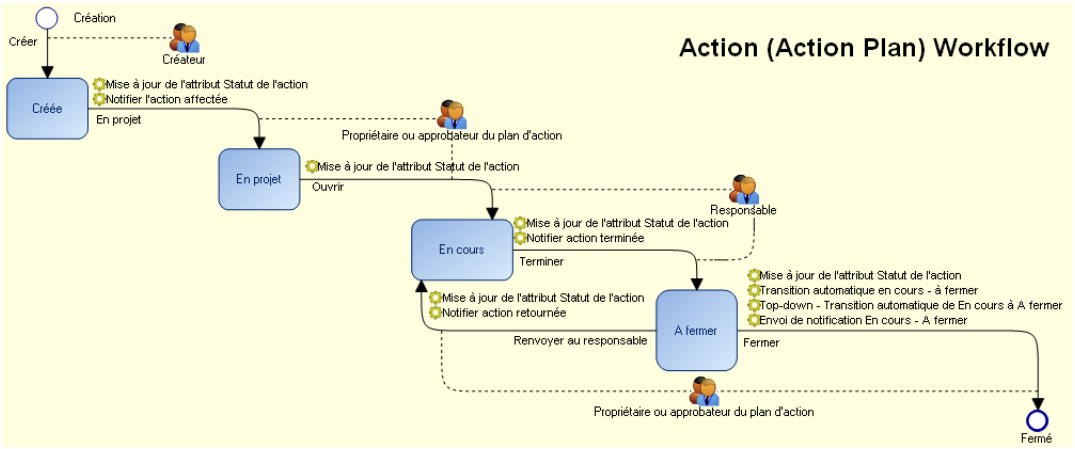
Après avoir consulté les rapports de suivi du plan d'action, l'approbateur peut :

- **Fermer** le plan d'action, qui maintient son statut à « Fermé » mais qui disparaît de la liste des tâches du créateur, approbateur et propriétaire.
- **Rouvrir** le plan d 'action, pour ajouter des actions. Le plan d'action reprend alors le statut « en cours ».

Workflow de plan d'action "top-down"



Workflows d'action



Les notifications sont envoyées par le créateur à l'utilisateur responsable :

- lorsqu'une action est assignée à un utilisateur
- lorsqu'une action est fermée.

DÉMONTRER LA CONFORMITÉ

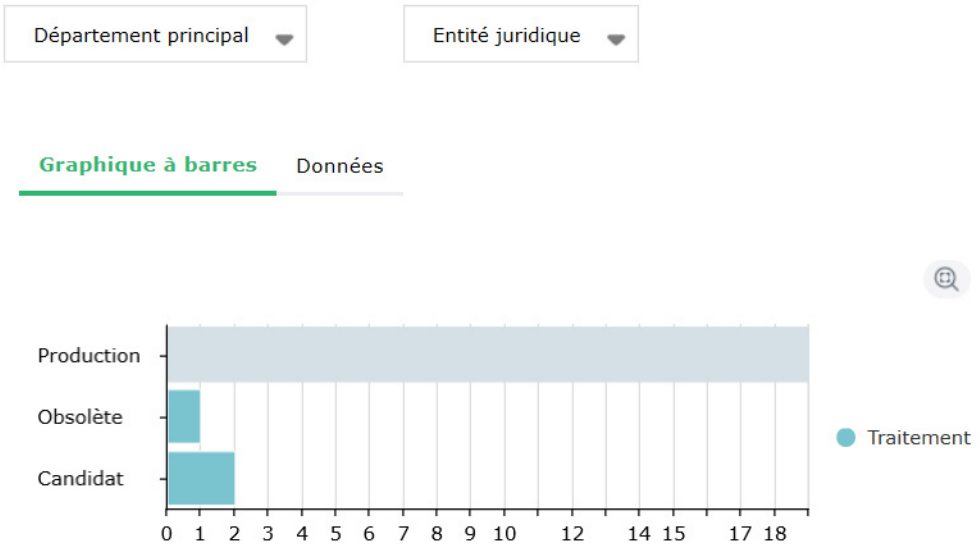
HOPEX Privacy Management vous permet de créer des rapports qui indiquent le niveau de conformité et de responsabilité des traitements.

Pour accéder aux rapports :

- Dans le menu de navigation, sélectionnez **Rapports**.

Statut du traitement

Ce rapport affiche l'ensemble des traitements, groupés par statut, pour identifier rapidement ceux qui nécessitent une validation.

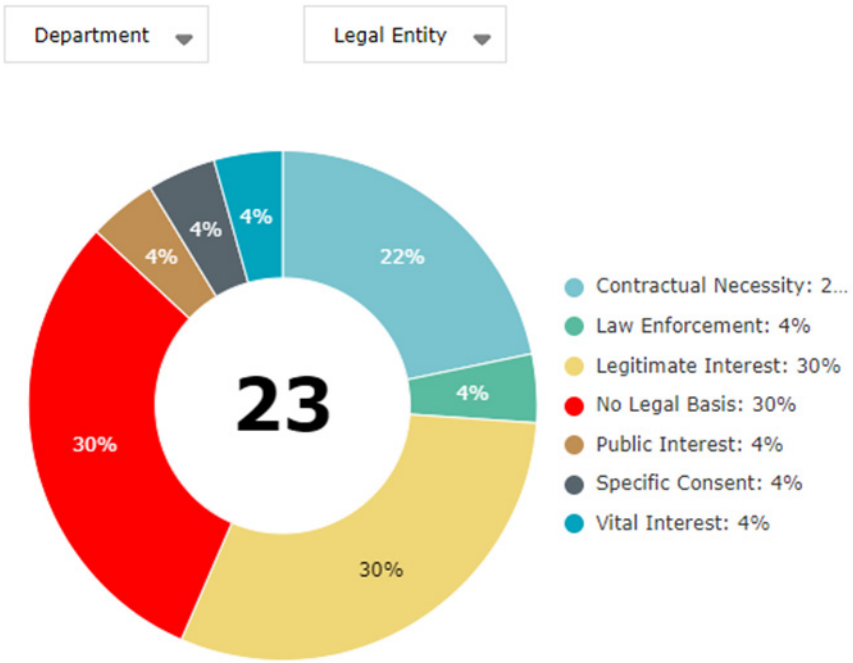


Pour rappel, les statuts suivants sont disponibles :

- Candidat
- Production
- Obsolète

Fondement juridique

Ce rapport affiche la répartition des traitements par fondement juridique. Il permet d'identifier les traitements pour lesquels aucun fondement juridique n'a encore été spécifié.



Activités sensibles

Le rapport permet d'identifier les traités impactés par des activités sensibles existantes.

Activité sensible	Traitement
Processing of data concerning vulnerable data subjects (EN)	Disciplinary Measures and Conciliation (EN)
	Disciplinary Measures and Conciliation (EN)
	Disciplinary Measures and Conciliation (EN)
	Employees evaluation process support (EN)
Processing of data on a large scale (EN)	Payroll Management (EN)
	Payslips and fees preparation (EN)
	Payroll Management (EN)
	Payroll Management (EN)
Processing of sensitive data or data of a highly personal nature (EN)	
Processing preventing data subjects' rights exercise (EN)	
Profilage	Email Marketing (EN)
	Financial Reporting (EN)
Surveillance systématique à grande échelle de zones publiques	Email Marketing (EN)

Registre des DPIA

Pour lancer ce rapport :

- Dans le menu de navigation, sélectionnez **Rapports > Rapports standards > Registre des DPIA**.

Ce rapport affiche les différentes DPIA réalisées sur les traitements auxquels vous avez accès. Il présente les informations suivantes :

- nom de l'évaluation
- nom du traitement
- DPO
- département
- niveau de conformité
- niveau de risque final
- date de clôture

Pour générer un document DPIA à partir d'une DPIA :

- Sélectionnez une DPIA et cliquez sur **Document DPIA**.

  ☛ *Pour plus de détails sur les DPIA, voir Réaliser une analyse d'impact (DPIA).*

Rapport de risques

Le DPO doit fournir un rapport sur le risque global et le niveau de conformité des traitements de l'organisation.

Pour lancer le rapport de risques :

- Dans le menu de navigation, sélectionnez **Rapports > Rapports standards > Rapport de risques**.

Le rapport contient deux tableaux :

- un pour les catégories de données

  ☛ *Pour plus de détails, voir Définir les catégories de données.*

- un autre pour les catégories de personnes concernées

  ☛ *Pour plus de détails, voir Définir les catégories de personne concernée.*

1. Rapport des catégories de données

Catégorie de données	Niveau de risque par défaut	Traitement	Evaluation préliminaire	Niveau de risque	Niveau de conformité	DPIA	Niveau de risque final
Biométriques	Elevée	Email Management (EN)	Yes (31/08/2020)	Très élevée	Non conforme	Yes (31/08/2020)	
Cookies et journaux système	Moyenne	Email Management (EN)	Yes (31/08/2020)	Très élevée	Non conforme	Yes (31/08/2020)	Moyenne
Financières	Elevée	Disciplinary Measures and Conciliation (EN)	Yes (28/11/2019)	Très élevée	Quasi-conforme	Yes (28/11/2019)	Moyenne
		Email Management (EN)	Yes (31/08/2020)	Très élevée	Non conforme	Yes (31/08/2020)	Moyenne
		Company car fleet management (EN)	Yes (28/11/2019)	Basse	Conforme	No	

Les deux rapports affichent le niveau de risque et de conformité qui s'appliquent à chaque catégorie de données et à chaque catégorie de personnes concernées. Les tableaux distinguent les résultats des évaluations préliminaires de ceux des DPIA.

☛ *Vous pouvez générer le rapport au format MS Word en cliquant sur l'icône correspondante dans le rapport.*

Transferts de données

Ce rapport affiche tous les transferts de données à caractère personnel, groupés par destinations, mettant en valeur l'envoi de données à caractère personnel vers des pays risqués.

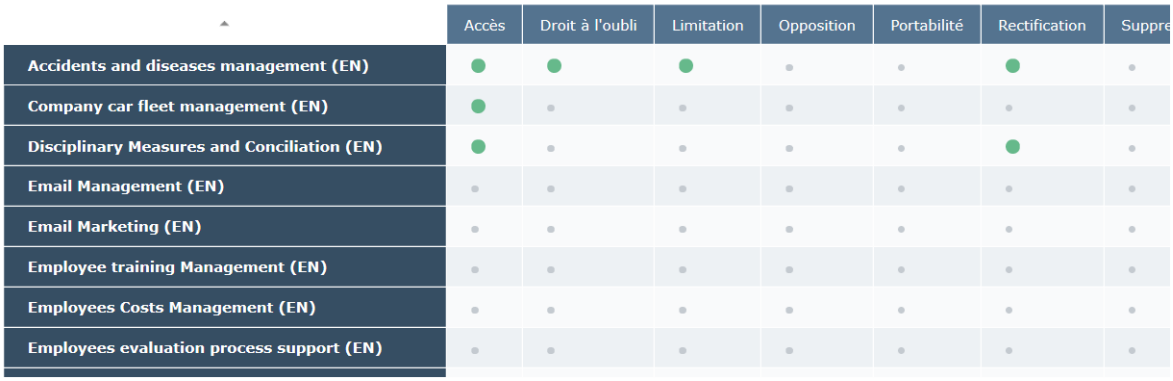
☛ *Pour construire la carte qui illustre des transferts de données, voir Carte des flux transfrontaliers.*

Rapport sur les droits des personnes concernées

Pour afficher un rapport sur les droits des personnes concernées :

- Dans le menu de navigation, sélectionnez **Rapports > Rapports standards > Droits des personnes concernées**.

Ce rapport contient la liste des traitements avec les droits des personnes concernées pris en compte.



	Accès	Droit à l'oubli	Limitation	Opposition	Portabilité	Rectification	Suppre
Accidents and diseases management (EN)	●	●	●	·	·	●	·
Company car fleet management (EN)	●	·	·	·	·	·	·
Disciplinary Measures and Conciliation (EN)	●	·	·	·	·	●	·
Email Management (EN)	·	·	·	·	·	·	·
Email Marketing (EN)	·	·	·	·	·	·	·
Employee training Management (EN)	·	·	·	·	·	·	·
Employees Costs Management (EN)	·	·	·	·	·	·	·
Employees evaluation process support (EN)	·	·	·	·	·	·	·

☛ *Pour plus de détails sur les droits des personnes concernées, voir Gestion des droits des personnes concernées et des informations.*

Rapport concernant les tiers

Ce rapport contient la liste des tierces parties impliquées dans les traitements existants.

Conditions préalables

Pour que les traitements s'affichent dans le rapport, vous devez avoir créé un élément de traitement de type « Tierce partie ».

Voir Créer un élément de traitement.

Lancer le rapport concernant les tiers

Pour lancer le rapport concernant les tiers :

- Dans le menu de navigation, sélectionnez **Rapports > Rapports standards > Rapport concernant les tiers**.

Contenu du rapport concernant les tiers

Pour chaque partie tierce le rapport fournit les informations suivantes :

- Traitement
- Risque brut
- Niveau de conformité
- Date de dernière évaluation du traitement

1. Active Third-Parties

Third-Party Name	Processing Activity	Raw Risk	Compliance Level	Last Assessment Date
Deloitte	Disciplinary Measures and Conciliation	Very High	Almost Compliant	11/28/2019
Salesforce	Accidents and diseases management	High	Poorly Compliant	8/30/2021

2. Obsolete Third-Parties

Third-Party Name	Processing Activity	Raw Risk	Compliance Level	Last Assessment Date

Le rapport distingue :

- les tierces parties actives
- Les tierces parties obsolètes

Registre des traitements

HOPEX Privacy Management vous permet de générer automatiquement le registre des traitements.

Voir Rapports associés aux traitements pour la description des rapports disponibles sur les traitements.

Carte des flux transfrontaliers

Pour générer la carte des flux transfrontaliers :

- Sélectionnez les transferts qui vous intéressent et cliquez sur .

Pour la description de ce rapport, voir Carte des flux transfrontaliers.

Applications informatiques

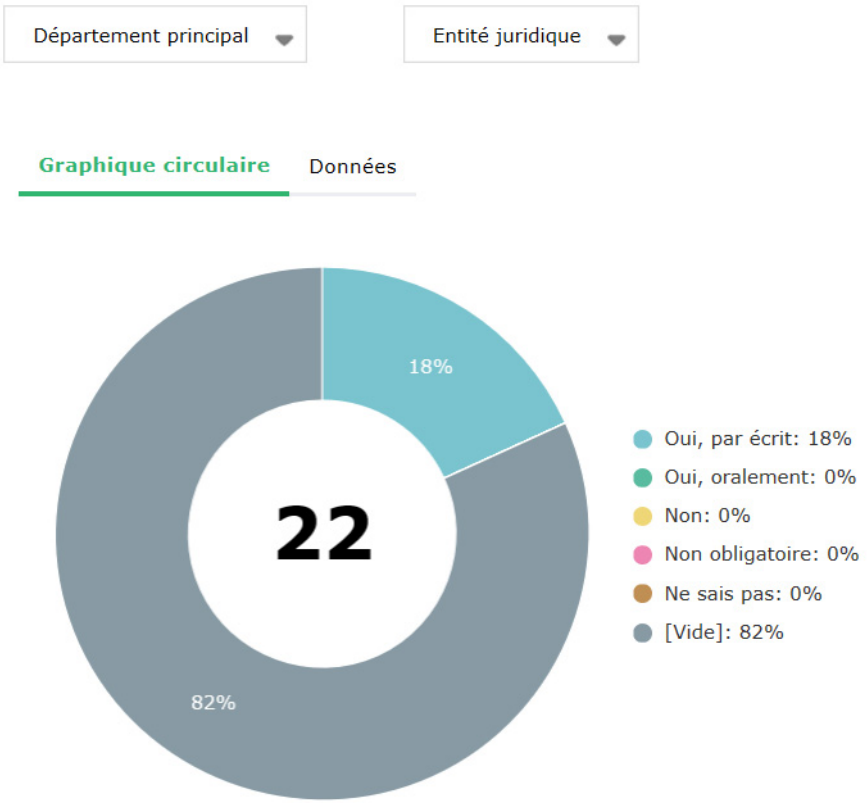
Ce rapport contient la liste de toutes les applications informatiques intervenant dans les traitements existants.

Processing Activity

Processing Activity	Processing Element	Application Name
Accidents and diseases management		
Company car fleet management		
Disciplinary Measures and Conciliation		
Email Management		
Email Marketing		
Employee training Management		
Employees Costs Management		
Employees evaluation process support		
Financial Reporting	Business Billing	Business Billing
Help Desk		
IT Logs Management	Privacy Application Processing	Business Billing
	Back-End Management	Back-End Management
IT systems administrators		

Informations

Ce rapport permet d'identifier les traitements pour lesquels aucune information n'a été fournie.

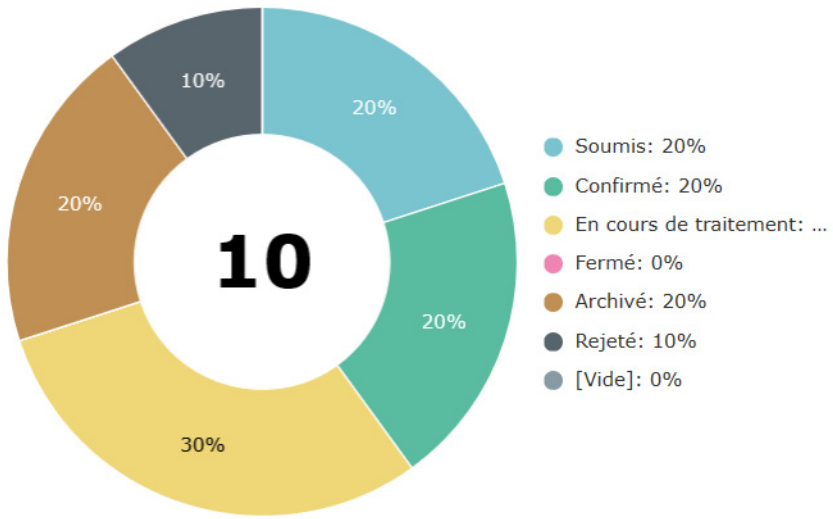


Violation des données

Ce rapport affiche l'ensemble des violations de données, groupées par statut, pour identifier facilement celles qui nécessitent une intervention immédiate.

Date de la détection | Date de la violation | Nbre heures depuis la détection

Graphique circulaire | Données



QUESTIONS FRÉQUENTES

A propos de la protection des données personnelles

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Différentes informations collectées ensemble peuvent conduire à l'identification d'une personne particulière et constituer des données personnelles.

Exemples de données personnelles :

- un prénom et un nom ;
- une adresse personnelle ;
- une adresse e-mail telle que prenom.nom@centreprise.com ;
- le numéro d'une carte d'identité ;
- une adresse IP (Internet Protocol)

☛ *Les données rendues anonymes ou un numéro d'enregistrement d'entreprise ne sont PAS considérées comme des données personnelles.*

Exemple de loi

Le Règlement général sur la protection des données (RGPD) est une loi européenne qui s'applique à tous les pays membres de l'union européenne depuis le 25 mai 2018.

Cliquez ici pour accéder à l'information officielle sur le RGPD.

Cliquez ici pour accéder au texte complet du règlement.

☛ *Ceci constitue un exemple seulement. **HOPEX Privacy Management** permet de prendre en charge toutes les lois concernant la protection des données.*

A propos des traitements

☛ *Pour des informations générales sur les traitements, voir Gérer les traitements.*

Pourquoi ne puis-je pas créer de traitement ?

Le responsable de la confidentialité doit vous avoir assigné un département.

Pour plus de détails, voir Relier des utilisateurs à un département.

Pourquoi le tableau de bord de mon traitement est-il vide ?

Les indicateurs affichés en haut de l'onglet **Vue globale** d'un traitement sont grisés/vides tant que vous n'avez pas fait d'évaluation préliminaire ou de DPIA sur le traitement.

Pour plus de détails, voir Tableau de bord du traitement.

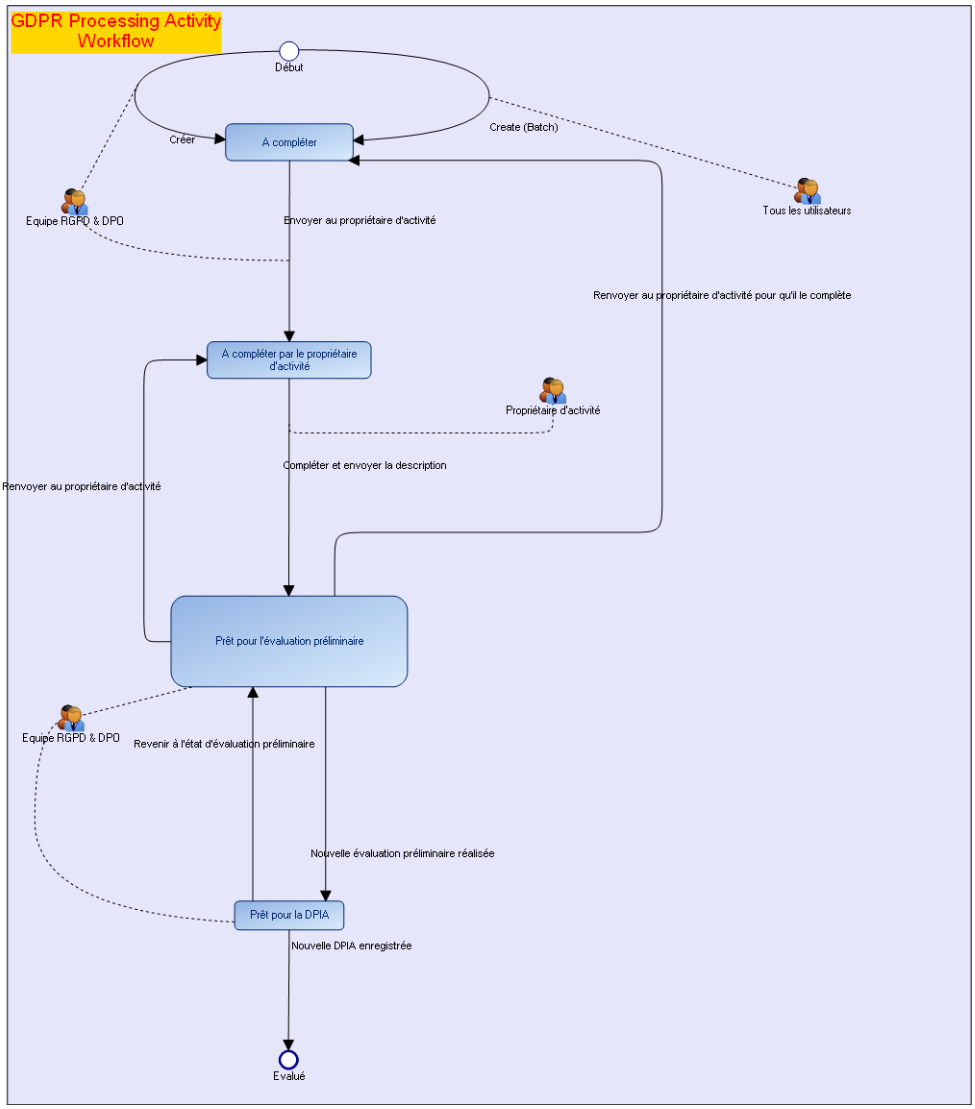
Comment produire un document Word de mon registre de traitements ?

Voir Créer un registre des traitements.

Une application intervient dans mon traitement. Je dois décrire spécifiquement comment cette partie du traitement est gérée. Que dois-je faire ?

HOPEX Privacy Management permet de décrire les éléments de traitement de type « application ». Pour plus de détails, voir Gérer les éléments de traitement.

Quelles sont les possibilités offertes par le workflow standard d'un traitement ?



A propos des évaluations

☛ *Pour plus de détails sur l'évaluation, voir Évaluer les traitements.*

Comment déterminer quels traitements doivent être évalués ?

Pour identifier les traitements à évaluer, nous vous conseillons d'étudier les éléments suivants :

- le ***niveau de conformité*** de vos traitements
  - Voir Visualiser le niveau de conformité initial d'un traitement.

    ☛ *Ces informations s'appliquent à un traitement qui n'a pas encore été évalué.*
  - Voir Consulter des rapports d'aide à la décision.

    ☛ *Ces informations concernent les traitements qui ont été évalués.*
- le ***niveau de risque final*** de vos traitements

  ☛ *Voir Consulter des rapports d'aide à la décision.*
- le ***statut d'évaluation*** (DPIA)

  ☛ *Voir Consulter des rapports d'aide à la décision.*

Est-il possible de réaliser une DPIA en dehors de la solution ?

Oui, c'est possible.

Nous vous conseillons de procéder de la façon suivante afin de référencer la DPIA en question dans **HOPEX Privacy Management** :

1. Créez la DPIA sans ajouter les risques et les recommandations.
2. Attachez la DPIA externe.
3. Remplissez les niveaux de validation et spécifiez les actions ultérieures à mener.

   ☛ *Pour plus de détails sur la création de DPIA, voir Réaliser une analyse d'impact (DPIA).*

Comment produire une version Word d'une DPIA ?

Vous pouvez générer un document Word de votre DPIA de deux façons :

- A partir de **Rapports > registre des DPIA**.

  ☛ *Pour plus de détails, voir Registre des DPIA.*
- A partir de l'onglet **DPIA** de la page de propriétés du traitement.

  ☛ *Pour plus de détails, voir Générer un document de DPIA.*

Certains de mes traitements sont similaires. Puis-je utiliser une DPIA existante ?

Oui, vous pouvez. Vous pouvez dupliquer un traitement puis effectuer les changements nécessaires.

☛ *Pour plus de détails, voir Réutiliser une DPIA.*

Comment est calculé le Niveau de conformité final ?

☛ *Ce champ est disponible dans la page **Evaluation préliminaire** ou **DPIA** d'un traitement. Voir Réaliser une évaluation préliminaire.*

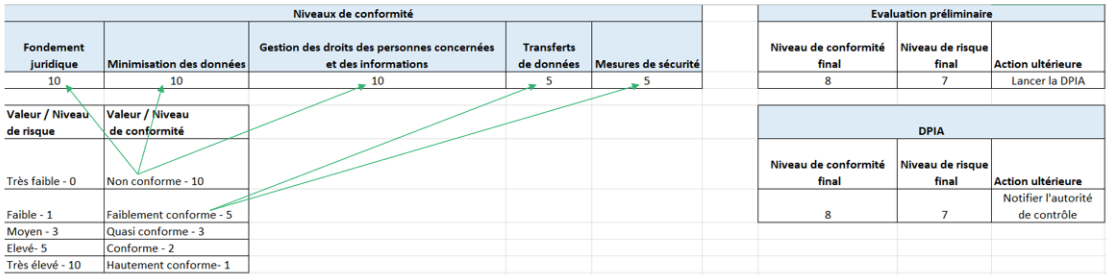
Voir aussi : Spécifier les niveaux de conformité.

Niveau de conformité final : somme des évaluations de conformité / 5. Le résultat est arrondi à l'entier supérieur le plus proche.

☛ *Les évaluations de conformité concernent les points suivants :*

- *Fondement juridique*
- *Minimisation des données*
- *Gestion des personnes concernées et des informations*
- *Transferts de données*
- *Mesures de sécurité*

Dans l'exemple ci-dessous, le niveau de conformité final = (10+10+10+5+5)/5 = 8



Niveaux de conformité				
Fondement juridique	Minimisation des données	Gestion des droits des personnes concernées et des informations	Transferts de données	Mesures de sécurité
10	10	10	5	5

Valeur / Niveau de risque	Valeur / Niveau de conformité
Très faible - 0	Non conforme - 10
Faible - 1	Faiblement conforme - 5
Moyen - 3	Quasi conforme - 3
Elevé- 5	Conforme - 2
Très élevé - 10	Hautement conforme- 1

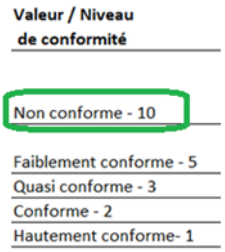
Evaluation préliminaire		
Niveau de conformité final	Niveau de risque final	Action ultérieure
8	7	Lancer la DPIA

DPIA		
Niveau de conformité final	Niveau de risque final	Action ultérieure
8	7	Notifier l'autorité de contrôle

Comparons le résultat obtenu avec les différentes valeurs possibles de niveau de conformité :

8 est plus proche de 10 (Non conforme) que de 5 (Faiblement conforme)

-> Niveau de conformité final = Non conforme



Comment est calculé le Niveau de risque final ?

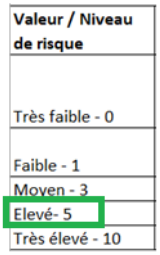
☛ *Ce champ est disponible dans la page **Evaluation préliminaire** ou **DPIA** d'un traitement. Voir Réaliser une évaluation préliminaire.*

Voir aussi : Comment est calculé le Niveau de conformité final ?

Niveau de risque final : Niveau de conformité final -1

Le résultat est arrondi à l'entier inférieur le plus proche.

Si Niveau de risque final = 7, alors Niveau de risque final = "Elevé" car 7 est plus proche de 5 (Elevé) que de 10 (Très Elevé)



Comment est calculé le champ Actions Ultérieures?

☛ *Ce champ est disponible dans la page **Evaluation préliminaire** ou **DPIA** d'un traitement. Voir Réaliser une évaluation préliminaire.*

Voir Comment est calculé le Niveau de risque final ?

Niveau de risque final (Evaluation préliminaire)	Valeur du champ "Actions ultérieures"
5	Lancer la DPIA
10	Lancer la DPIA
Autre valeurs	Autre

Niveau de risque final (DPIA)	Valeur du champ "Actions ultérieures"
5	Notifier l'autorité de contrôle
10	Notifier l'autorité de contrôle
Autre valeurs	Autre

A propos des transferts

Comment créer des transferts ?

Les transferts doivent être créés dans l'onglet **Détails** d'un traitement.

Y a t-il un moyen de visualiser graphiquement les transferts ?

Oui, **HOPEX Privacy Management** vous permet d'afficher une carte des flux transfrontaliers pour un traitement particulier.

Pour plus de détails, voir :

- Carte des flux transfrontaliers.
- Spécifier les transferts de données sur un traitement.

J'ai créé des transferts mais je ne peux pas afficher la carte des flux transfrontaliers. Quel est le problème ?

Voir Conditions préalables à l'utilisation d'une carte des flux transfrontaliers.

☛ *Veillez également à rafraîchir le rapport après avoir créé les transferts sur les traitements.*

A propos de l'import et de l'intégration avec HOPEX

Comment réutiliser les informations provenant d'autres solutions HOPEX?

HOPEX Privacy Management permet de :

- Importer des applications et processus
- Les réutiliser pour créer des traitements

  ☛ *Pour plus de détails, voir Pour créer un traitement directement dans HOPEX Privacy Management :.*
- Visualiser les propriétés des applications/processus et des diagrammes associés directement à partir de **HOPEX Privacy Management**.

Je n'arrive pas à glisser-déposer un sous-processus sous un département. Quel est le problème ?

Il est possible de glisser-déposer des sous-processus sous un département afin de créer un traitement, mais il existe une règle pour cela :

Lorsque vous faites glisser un sous-processus sous un département, c'est le processus parent qui est déplacé sous le département (pas le sous-processus).

Prenons un exemple pour mieux illustrer ce cas. Imaginons que :

- sous l'arbre de gauche, vous avez 3 sous-processus sous un processus.

- vous glissez-déposez l'un de ces sous-processus sous un département de l'arbre de droite.

Dans l'exemple ci-dessus, le processus « Recruter des collaborateurs » donne naissance au traitement « Gérer les Ressources Humaines ».

A présent vous voulez glisser-déposer un autre sous-processus sous un autre département. Dans notre exemple vous pouvez glisser « Gérer les compétences et la formation des collaborateurs » sous « Finance ».

- > Un message d'erreur vous signale que le processus « Gérer les Ressources Humaines » ne peut générer de traitement parce qu'il est déjà associé à un traitement.

Divers

Est-il possible de visualiser le diagramme d'un processus importé ?

Oui c'est possible lorsque le diagramme a été importé avec le processus.

Pour ce faire :

1. A partir du menu de navigation, cliquez sur **Traitements**.
2. Ouvrez la page de propriétés du traitement.
3. Cliquez sur l'onglet **Détails** puis sur **Vue de détails**.
   A côté du traitement ou sous-traitement concerné, un bouton qui permet d'afficher le diagramme est mis à disposition.

   ☛ *Vous pouvez aussi accéder au site Web statique d'un processus s'il a été importé dans **HOPEX Privacy Management**.*

Mon organigramme des DPO est vide. Que dois-je faire ?

Vous pouvez construire l'organigramme des DPO en spécifiant la hiérarchie des DPO dans les pages de propriétés de l'entité.

Voir Définir les propriétés des entités. Vous devez remplir les champs **DPO** et **Reporting au DPO** pour que l'organigramme puisse être généré de façon automatique.

Je ne peux pas créer d'entités juridiques. Que dois-je faire ?

Seul le responsable de la confidentialité peut créer des entités juridiques et des départements.

Assurez-vous que vous êtes connecté avec ce profil.

GLOSSAIRE DE LA PROTECTION DES DONNÉES PERSONNELLES

Action	Une action fait partie d'un plan d'action et représente une transformation ou le traitement par une organisation ou un système.
Activité sensible	Une activité sensible est une activité dont l'impact global sur le risque du traitement est important.
Archive physique	Une archive physique correspond aux locaux dans lesquels l'historique des archives est conservé.
Autorité de contrôle	Une autorité de contrôle est une autorité publique établie par un état membre. Elle peut être contactée par l'entité juridique dans le but de, par exemple, notifier une violation de données ou faire un retour concernant la DPIA d'un traitement.
Autorité de protection des données	Une autorité chargée de la protection des données est une autorité nationale dont la tâche est d'assurer la protection et la confidentialité des données, ainsi que de surveiller et de faire appliquer les réglementations concernant la protection des données au sein de l'Union Européenne.
Cadre réglementaire	Un cadre réglementaire représente un ensemble de directives contraignantes ou non, définies par un gouvernement dans le cadre d'une loi, par un groupement professionnel sous forme de bonnes pratiques ou en interne par une organisation.
Catégorie de données	Les catégories des données sont utilisées dans le but de regrouper différentes données à caractère personnel.

Catégorie de personne concernée	Une catégorie de personne concernée est un type de partie prenante qui interagit avec votre organisation dans l'environnement d'entreprise (par exemple un client du secteur privé, un fournisseur).
Co-responsable du traitement	Les co-responsables de traitement peuvent déterminer conjointement les finalités et les moyens du traitement.
Consentement	Le consentement est une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Correspondant DPO	Un correspondant DPO peut être amené à assister le DPO dans les grandes entreprises.
Correspondant informatique	Le correspondant informatique est chargé d'assurer le support informatique.
Demande en provenance de la personne concernée	Une demande de personne concernée est une demande formelle adressée à un responsable de traitement pour qu'il intervienne sur ses données à caractère personnel.
Document de politique interne	Les documents de politique interne permettent de joindre des documents ou de spécifier une URL à utiliser dans le but de fournir des preuves de la responsabilité de l'entreprise.
Données à caractère personnel	Les données personnelles comprennent les informations relatives aux personnes physiques ou « personnes concernées », et pouvant être utilisées directement ou indirectement pour identifier une personne.
DPIA	L'analyse d'impact relative à la protection des données (DPIA - Data Protection Impact Assessment) est une analyse d'impact relative à la confidentialité des données, dont l'objectif est d'identifier et d'analyser comment certaines actions ou activités peuvent affecter la vie privée. Dans le cadre de lois sur les données à caractère personnel, les analyses d'impact relatives à la protection des données sont obligatoires dans certains cas, tels que le profilage.
Droit à l'oubli	Le droit à l'oubli est également appelé Droit à l'effacement. Il autorise la personne concernée à faire supprimer ses données à caractère personnel par le responsable de traitement, à stopper la dissémination de ses données, et à interdire leur traitement par des tiers.
Droit d'accès	Le droit d'accès permet aux personnes concernées d'accéder aux données à caractère personnel les concernant et que le responsable de traitement détient.

Effacement des données	Voir Droit à l'oubli.
Entité juridique	Une entité juridique est une entreprise ou organisation qui a des droits et obligations juridiques.
Établissement	Un établissement correspond à la localisation (site) d'une entité juridique.
Exigence	Une exigence est un besoin ou une attente explicitement exprimés, imposés comme contrainte à respecter dans le contexte d'un cadre réglementaire.
Finalité	La finalité d'un traitement est l'objectif principal de ce traitement. Exemples : enquête de satisfaction, gestion des clients, surveillance d'un site
Garantie	Les garanties sont des mesures prises pour assurer la légitimité des flux de données. Les garanties s'appliquent aux transferts seulement.
Mesure de sécurité	Les mesures de sécurité sont des mesures techniques et organisationnelles appropriées à prendre pour s'assurer que les exigences de la réglementation sont satisfaites.
Minimisation	La minimisation est un principe selon lequel les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
Ordinateur	Un ordinateur est un matériel qui peut héberger et exécuter un logiciel. Conjointement avec les applications qu'il héberge, il fournit les services d'information et de données.
Organigramme	Un organigramme contient la structure hiérarchique des DPO de l'organisation. Il montre les relations entre les DPO qui ont été nommés et permet d'identifier les responsabilités de chacun au sein de l'organisation. Il est automatiquement construit en se fondant sur les informations saisies sur les entités juridiques.
Période de conservation	Une période de conservation permet de consigner la période pendant laquelle les données à caractère personnel seront stockées par l'organisation.
Personne concernée	Une personne concernée est une personne physique dont les données à caractère personnelles font l'objet d'un traitement par un responsable de traitement ou un sous-traitant.
Plan d'action	Un plan d'action comprend une série d'actions, son objectif étant de réduire les risques et événements ayant un impact négatif sur les activités de l'entreprise.

Portabilité des données	La portabilité est l'exigence pour les responsables de traitement de fournir à toute personne concernée une copie de ses données dans un format permettant à un autre responsable de traitement d'en faire usage.
Profilage	Le profilage comprend toute forme de traitement automatisé de données à caractère personnel dont le but est d'évaluer, analyser, ou prédire le comportement des personnes concernées.
Propriétaire de traitement	Le propriétaire de traitement fournit une description détaillée du traitement. Il ne participe pas à l'évaluation du traitement.
Protection de la vie privée dès la conception	La protection de la vie privée dès la conception est un principe qui introduit la protection de la vie privée dès la phase de conception des systèmes (plutôt que de l'introduire a posteriori).
Registre des traitements	Le registre des traitements doit contenir des informations significatives concernant le traitement des données, par exemple les catégories de données, les groupes de personnes impactées, la finalité du traitement et les destinataires des données. Il doit être mis à disposition des autorités à leur demande.
Règles internes de l'entreprise (BCR)	Les BCR sont un ensemble de règles contraignantes permettant aux entreprises et organisations multinationales de transférer des données à caractère personnel, de l'UE vers leurs affiliés hors de l'UE (mais faisant partie de l'organisation).
Représentant	Un représentant est une personne de l'Union Européenne désignée explicitement par le responsable de traitement pour servir de point de contact auprès des autorités de contrôle.
Représentant National	Un représentant national est un représentant de l'entité juridique dans l'un des états membres. Une entité juridique n'appartenant pas à l'Union Européenne doit nommer des représentants dans chaque état membre dans lequel l'entité traite des données à caractère personnel.
Responsable de la protection des données	Le DPO (Data Protection Officer) ou Responsable de la protection des données travaille de manière indépendante pour s'assurer de la bonne application des textes juridiques concernant les lois de protection des données.
Responsable de traitement	Le responsable de traitement est l'entité qui définit les finalités, conditions et moyens du traitement des données à caractère personnel.

Risque	Un risque représente un risque relatif à la protection des données qui doit être identifié et évalué au cours d'un DPIA.
Sous-traitant	Un sous-traitant est l'entité qui traite des données à caractère personnel pour le compte du responsable de traitement.
Tiers	Un tiers est une personne physique ou morale, une autorité publique, un service ou un organisme autre qu'une personne concernée, un responsable de traitement, un sous-traitant et les personnes qui, placées sous l'autorité directe du responsable de traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.
Traitement	Un traitement est une opération réalisée sur les données à caractère personnel, de manière automatisée ou manuelle, comprenant la collecte, l'utilisation, l'archivage, etc.
Transferts de données	Dans le cadre d'une loi sur la protection des données personnelles, un transfert de données est un transfert ou une copie de données à caractère personnel.
Violation des données à caractère personnel	Une violation de données personnelles est une faille de sécurité conduisant à un accès accidentel ou illicite, à la destruction, à l'utilisation abusive de données à caractère personnel.

APPENDIX: GDPR IN DETAILS

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

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

TERRITORIAL SCOPE

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

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

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

Establishment Principle in the Directive

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

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

Establishment in Different States

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

Company Chain

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

Reference

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

Establishment Principle in the Regulation

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

Establishment Notion

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

Effectiveness

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

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

Stability

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

References

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

2. Recital (22) Regulation 2016/679

Foreign Company Subject to Regulation

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

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

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

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

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

Offering of Goods or Services to EU residents

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

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

Monitoring Behavior of EU residents

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

Controller Representative or Foreign Processor

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

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

Obligation is excluded if

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

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

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

Applicability Member State Law due to International Law

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

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

Reference

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

PERSONAL DATA PROCESSING

Legal Entity Data

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

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

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

Common Data

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

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

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

Special Categories of Data

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

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

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

Sensitive Data

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

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

Legitimate Conditions for Sensitive Data

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

Biometric Data

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

Genetic Data

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

Health Data

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

Sanction for Sensitive Data Breaches

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

Common Data

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

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

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

Sensitive Categories of Data

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

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

Sensitive Data

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

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

Legitimate Conditions for Sensitive Data

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

Biometric Data

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

Genetic Data

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

Health Data

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

Sanction for Sensitive Data Breaches

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

GDPR LEGAL ROLES

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

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

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

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

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

The Undertaking

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

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

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

The Enterprise as an Interested Subject

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

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

SMEs as data controllers

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

Derogations and Facilities for SMEs

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

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

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

NOTICE AND CONSENT

Transparency

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

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

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

Notice:Contents

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

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

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

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

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

Notice:New Rules

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

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

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

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

Sanctions for omitted notice

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

Notice:Exceptions

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

Personal data collected from data subject

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

Personal data not obtained from the data subject

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

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

Notice:When to be Issued

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

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

- when collecting data, (Article 13.1).

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

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

Consent

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

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

Sanctions for consent violations

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

Consent Lawfulness Conditions

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

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

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

RIGHTS OF DATA SUBJECTS

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

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

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

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

Access Right

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

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

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

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

Right to Rectification

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

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

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

Right to Erasure

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

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

Right to be Forgotten

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

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

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

Right to be Forgotten: History

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

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

The ECJ has found it unlawful that events that have long since passed can continue to be offered to the internet reader as news of the day, even though they are decontestualized and no longer topical; Regulation 2016/679 now provides precise regulatory support without the need for interpretative reconstructions through the provision contained in art. 17.

Right to Restriction of Processing

In some circumstances, the data subject has the right to obtain a restriction of the processing (Article 18).

The cases of exercise of the right to restriction of processing are when one of the following applies:

- the data subject contests the accuracy of the personal data, for the period required to verify the data accuracy [art. 18.1, a)];
- the processing is unlawful and the data subject opposes the erasure and asks for restriction as an alternative [art. 18.1, b)];
- with the processing ceased, the data subject needs the data to exercise his/her own right to trial [art. 18.1, c)];
- the data subject has objected the processing for legitimate reasons, pending the necessary verifications [art. 18.1, d)].

Portability Right

Of particular importance is the new right to portability (Article 20) which gives the data subject the power to obtain his/her personal data from the Controller in an "open" format, easily usable on the most widely used platforms: another "bridge" launched between the world of data protection and the increasingly contiguous one of the competition.

Where the legal basis of the processing is given by the consent or execution of a contract and the processing is carried out by automated means, the right to portability includes the right of the data subject to obtain the direct transmission of his personal data from one Controller to the other, if technically feasible (Article 20.2).

Free Exercise of Rights

The exercise of all data protection rights is normally free, both for the information provided and for the actions taken (Article 12.5).

Exception is the case where «requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character», in which case the Controller may charge a reasonable fee on the administrative costs incurred or refuse to process the request. In such a case, the burden of proof of the manifestly disproportionate nature of the claim is on the Controller.

If, in general, the Controller refuses to comply with the requests of the data subject, he must inform him of the reasons and the possibility for the data subject to file a

complaint with the National Supervisory Authority and to apply to the ordinary judicial authority (Article 12.4) .

Right to Object

Where the processing is necessary for the execution of a public interest task or for the pursuit of a legitimate interest of the data controller or a third party, the data subject has the right to object to the processing of his/her personal data in the presence of legitimate reasons related to his/her particular circumstances.

As already provided in Directive 95/46/EC, the objection to the use of personal data for direct marketing purposes is fully discretionary (Article 21.2).

GDPR Documentation System

The Regulation changes the axe for the legitimacy of the processing of personal data, moving it from the so-called legitimacy requirements1 to the compliance data protection system and the direct attribution of responsibility to the data controller.

In summary, the Regulation stipulates that compliance with the obligations of the data controller – for whose satisfaction he is therefore responsible and he is required to demonstrate it – can be expressed as follows:

- through a documentation system consisting in the maintenance of the record of processing activities, descriptive of the processing carried out under its own responsibility (Article 30) and further compulsory documentation
- the adoption of appropriate policies (Article 24) and compliance assessments with regard to processing and effectiveness assessments concerning the data protection measures implemented
- adherence to approved Code of Conducts (Articles 24.3, 28.5, 32.3)
- the use of a certification mechanism (Articles 24.3, 25.3, 28.5, 32.3).

Therefore, documentation requirements, assessments and compliance with codes of conduct and data protection certification systems are tools to demonstrate compliance of the company with legal requirements.

Records of Processing

The obligation of documentation has its core in the register of processing (Article 30).

Specifically, the document must contain the following information:

- contact data of the Data Controller, eventual joint-controllers, national representatives and data protection officer [art. 30.1, lett. a)];
- purpose of the processing [art. 30.1, lett. b)]
- categories of data subjects and the categories of data referred to them [art. 30.1, lett. c)]
- categories of recipients to whom data are transmitted (including recipients in third countries) [art. 30.1, ch. d)]
- third countries to which personal data and related processing operations are transmitted together with the documentation of the appropriate security measures when the transfer is based on the legitimate interests of the data controller [art. 30.1, lett. e)]
- where possible, retention periods for the different categories of data used [art. 30.1, lett. f)]
- where possible, a general description of the adopted technical and organizational security measures [art. 30.1, lett. g)].

This documentation, which should also be prepared by the Processor (Article 30.2), must be submitted to the National Supervisory Authority, upon request (Article 30.4).

Supporting Documentation

The system documentation is completed by the following "supporting documentation", for which GDPR requires the conservation and management:

- Documentation on the relationship between "joint-controllers" (Article 26)
- Contractual determination of the relationship between Controller and Processor and related obligations (Article 28.3)
- Violation of Personal Data, i.e. data breaches (Article 33.5)
- Appropriate assessments and guarantees regarding foreign data transfers based on the legitimate interest pursued by Controller or Processor (Article 49.6)1.

1. In a version of the proposed Regulation prior to that published on 21/1/2012, supporting documentation for foreign data transfers was also required, based on standard data protection clauses or binding corporate rules (Article 39.3).

Abolition Obligation Notification

The obligation to maintain the system documentation under the responsibility of the data controller replaces the previous obligation to notify the Authority laid down in the Directive 1.

1. See Section IX, Articles 18 and subsequents, Dir. 95/46/EC.

Sanction for Violation of Documentation

The vioaltion of obligations regarding proper management and retention:

- of the register of processing activities
- of supporting documentation regarding any breaches of personal data and assessments of foreign data transfers made on the basis of the legitimate interest of the Controller

is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Prior Consultation to Supervisory Authority

The Controller must consult the national supervisory authority prior to processing, if the impact assessment referred to in Article 35 reveals that the processing itself would pose a high risk in the absence of proper measures adopted by the Controller to mitigate the risk (Article 36).

Sanction for Omitted Prior Consultation

Violation of the prior consultation obligation is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.4).

DATA PROTECTION ASSESSMENT

When a data processing poses specific risks, it is subject to a preliminary impact assessments (DPIA).

DPIA

When it is likely that the processing, by its nature, its object or purposes, entails "high risks to the rights and freedoms" of the data subject, the data controller will have to carry out an ex ante evaluation of the impact that the processing may have from a data protection perspective: this is the so called Data Protection Impact Assessment (DPIA). The obligation laid down in Article 35 constitutes the manifestation of the accountability of the Controller (Articles 5.2 and 24) where, by means of a prior assessment, specific risks to the rights of the data subjects are encountered, caused by the usage of «new technologies, and taking into account the nature, scope, context and purposes of the processing».

Sanction for Omitted DPIA

Violation of the obligation for the Controller to carry out the data protection impact assessment (DPIA) is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Supervisory Authority Consultation

Regulation 2016/679 has given mandate to the individual national authority to identify the types of processing that require to carry out such an assessment (Article 35.4).

TECHNICAL AND ORGANIZATIONAL MEASURES

Security Measures

Security is in itself a micro-system within the broader data protection scenario (Article 32). Technical and organizational measures play a fundamental role according to the Regulation, at least under six distinct profiles:

- They determine the level of security adopted (Article 32)
- They must allow the Controller to adequately protect the data from any breach (Article 33) and to allow it to react promptly in the event of a breach
- They must be able to adequately support the exercise of the data subjects' rights (eg Article 17.2)
- They must be able to reduce the risks associated with the protection of personal data [eg. art. 22.2, b)]
- Depending on their type and quality, they affect the risk assessment
- They constitute an important organizational criterion in the management of controllers, agents, subcontractors (eg articles 24.1, 28.1, 28.4)
- They allow verification and demonstrate the accountability level of the Controller [eg Art. 25.1, 30.1 g), 30.2 d)].

Failure to take appropriate security measures is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Security in General

Regardless of Italian legislation (Dlgs 196/2003), the GDPR does not require specific security measures, albeit minimal, but imposes a generic obligation on both the Controller and the Processor, to take measures to mitigate the risks associated with the data processing (Article 32). This, as stated below, involves the requirement for an initial assessment of adequacy between risks and measures for the Company; since the measures taken must ensure an appropriate level of security, given the state of the technology and the related costs.

The provision of Article 32 concerns, in addition to "technical" measures, those of an organizational nature; both must be the result of a risk analysis.

Security Assessment

Determining the measures to be taken requires a complex evaluation process.

The estimate of their adequacy must be based on the analysis «the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons» (art. 32.1).

In addition, the risks to be assessed are those presented by «accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed» (art. 32.2).

According to the principle of accountability (Article 24), the Controller must take into account the validity of his assessments.

DATA BREACH

Security Measures against Data Breaches

The organizational and technical measures mentioned in the Regulation are the cornerstone of the discipline: they concern both the most appropriately technical measures (such as authentication credentials, authorization profiling system, encryption, antivirus and back up etc.) and the organizational ones (such as contractual regulation of relationships with those data processors, confidentiality constraints and instructions given to individuals who work on data, policies and records of processing, etc.). One of the interaction profiles of organizational and technical measures with the security system is to protect and respond to personal data breaches.

The declination of organizational and technical measures in the information security system

Technical-organizational measures interact with the entire system for the protection of personal data under different profiles:

- As a system of protection and reaction to violations (data breach)
- As verification and demonstration of compliance (accountability)
- As a tool for reducing risk (minimizing data, pseudonymization, privacy by design)
- As a Risk Assessment Component (DPIA)
- As organizational measure (contractual constraints with processors, confidentiality of people managing data, policies and registers)
- As a way of faacilitating the exercise of rights (opposition, forgiveness or cancellation, limitation of processing, portability, profiling and automated decisions).

Prevention and reaction to data breaches

The security measures objectives – found in the Regulation – are dual:

- of an "active" or a preventative nature, consisting in reducing the risk of unauthorized destruction, loss, modification, disclosure or accidental or unlawful access to personal data
- of a "passive" or "reactive" nature, consisting in a prompt response to incidents in the implementation of effective remediation actions and timely communications to the competent authorities, data subjects and the Controller (if the incident concerns the Processor).

The criterion of adequacy of the measures

The "active" protection profile requires the adoption of an adequate security level. The determination of the adequacy of the level is achieved adopting a risk-based approach: «appropriate technical and organisational measures to ensure a level of

security appropriate to the risk» should be implemented, «taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons» (Article 32 (1)).

The legislator provides an example list of such measures that may include:

- «(a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.».

Data breach incidents

On the "reactive" front, in addition to system resilience and recovery policies, the legislator imposes specific disciplines in case of data breaches.

The state of the law

It should be noted that, according to EU Regulation no. 611/2013, concerning publicly available electronic communications providers, encryption or hashing systems are not considered to be comprehensive remedies for protection against the risk of infringement, as they must be accompanied by appropriate organizational and technical measures under art . 17 of Directive 95/46 [Recital (17)]. However, they allow – if they comply with the conditions laid down – to avoid notifying users in case of a breach (see Article 4).

Cybersecurity Directive

The so-called Cybersecurity Directive is being published on the Official Journal of the European Union. The Directive envisages for energy, transport, banking, financial market infrastructure, health and water supply services:

- the adoption of security measures to manage the risks to the networks and information systems that they control and use in their respective activities
- the notification to the competent authorities of those incidents having a significant impact on the continuity of the essential services they provide.
- These provisions should be harmonized with the corresponding ones contained in the Regulation on the processing of personal data.

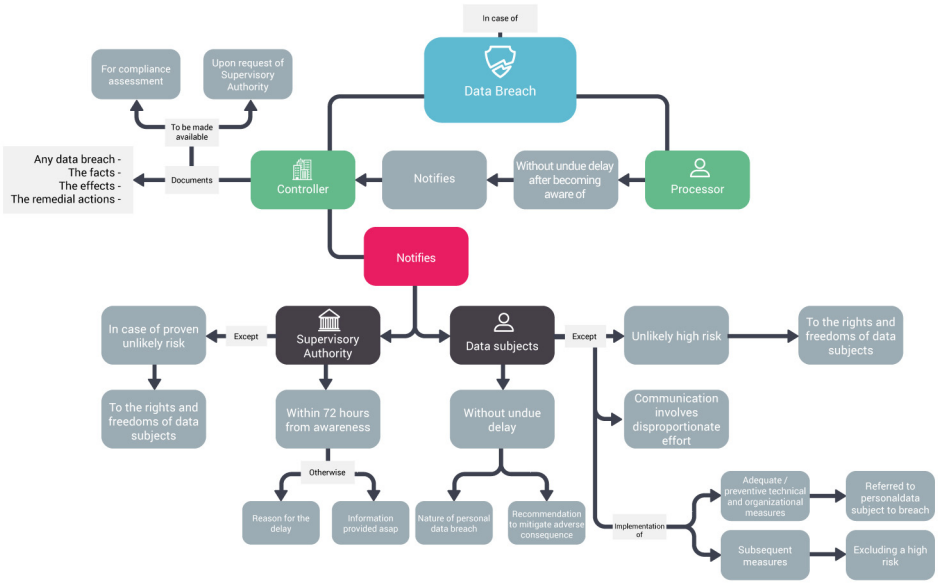
GDPR

The Regulation extends the reporting obligations for personal data breaches to their respective competent authorities, to all Data Controllers. The notification must be made without unjustified delay and, in any case, within 72 hours of the date on which it has become known, unless the Controller demonstrates that it is unlikely that the data breach would present a risk to the rights and freedoms of the data subjects affected by the breach. If the notification takes place after the 72-hours

deadline, the reasons for the delay must be explained [Recital (67) and art. 31]. In the event of a high risk for the rights and freedoms of the data subjects, notification should also be made to the latter, by making recommendations to mitigate potential adverse effects. Notification to data subjects must be carried out «as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities» [Recital (86)].

Adopting appropriate technical measures to effectively limit the risk of identity theft or other forms of abuse positively affects the consequences of a data breach and the resulting legal implications.

Personal Data Breach



Personal Data Breach
Regulation (EU) n.2016/679

Sanction for Sensitive Data Breach

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

DATA TRANSFER ABROAD

The flow of personal data

- from a country belonging to the European Union or the European Economic Area (EEA, ie outside the territories of all EU Member States beyond Norway, Iceland and Liechtenstein)
- to another country

is subject to specific rules to ensure that the protection granted to personal data under European law is not affected by transferring the same data to a country without a system of safeguards considered similar to that guaranteed in the EU.

1.1. Countries that offer personal data protection system, considered appropriate by the EU Commission

The external flow of personal data between

- a country of the European Economic Area (or EEA) and
- an extra-EU country

is considered legitimate and free if the European Commission has previously recognized with its own formal decision that there is a data protection system at the receiving country which offers personal data a protection similar to what they enjoy under EU law.

1.2. Countries not on the list of those with "adequate protection"

In the event that the receiving country is not included in the list of data protection adequate countries, a legal ground must be identified that makes such transfer legitimate. One of these legitimacy conditions that can be used effectively in transactions concerning the Company's relationship with Third Parties is the use of contractual terms binding the Company and the receiving Third Party to the same guarantees as provided by EU law for the protection of personal data. In this way, the obstacle to the non-applicability of EU law to the non-EU third-party is overcome, binding the Third Party to contractual requirements comparable with the rules set forth by the law.

For this legitimacy requirement to go beyond the ban on the transfer of personal data to countries without adequate protection, the contractual clauses used must be exactly the same as those officially approved by the EU Commission without any modifications.

1.3. The various contractual models approved by the EU Comission

In this respect, the Commission has, over the years, approved several sets of standard contractual clauses dealing with the following cases:

- Personal data flows between the EU Controller (the data exporter) and the Extra-EU Controller (the data importer)
- Personal data flows between the EU Controller (the data exporter) and the Extra-EU Processor (the data importer)
- Personal data flows between Data Processor and Data Processor.

SANCTIONS AND DAMAGES

New Sanctions

The extent of administrative sanctions (up to 4% of the total annual turnover – Article 83) suggests revising the data protection risk assessment approach, in order to update it and adjust the risks determination.

Sanction for Sensitive Data Breaches

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

Sanction for Omitted Prior Consultation

Violation of the prior consultation obligation is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (Article 83.4).

Sanction for Omitted DPIA

Violation of the obligation for the Controller to carry out the data protection impact assessment (DPIA) is sanctioned with administrative fines of «up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher» (art. 83.4).

Sanction for Consent Violations

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

Sanction for Rights Violations

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

GDPR-RELATED DEFINITIONS

Binding Corporate Rules (BCRs) - a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation)

Biometric Data - any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification

Consent - freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Concerning Health - any personal data related to the physical or mental health of an individual or the provision of health services to them

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

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

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject - a natural person whose personal data is processed by a controller or processor

Delegated Acts - non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity

Derogation - an exemption from a law

Directive - a legislative act that sets out a goal that all EU countries must achieve through their own national laws

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Enterprise - any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

Filing System - any specific set of personal data that is accessible according to specific criteria, or able to be queried

Genetic Data - data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual

Group of Undertakings - a controlling undertaking and its controlled undertakings

Main Establishment - the place within the Union that the main decisions surrounding data processing are made; with regard to the processor

Personal Data - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution

Recipient - entity to which the personal data are disclosed

Regulation - a binding legislative act that must be applied in its entirety across the Union

Representative - any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities

Right to be Forgotten - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Supervisory Authority - a public authority which is established by a member state in accordance with article 46

Trilogues - informal negotiations between the European Commission, the European Parliament, and the Council of the European Union usually held following the first readings of proposed legislation in order to more quickly agree to a compromise text to be adopted.