

HOPEX GDPR

Guide d'utilisation

HOPEX V2R1



Les informations contenues dans ce document pourront faire l'objet de modifications sans préavis et ne sauraient en aucune manière constituer un engagement de la société MEGA International.

Aucune partie de la présente publication ne peut être reproduite, enregistrée, traduite ou transmise, sous quelque forme et par quelque moyen que ce soit, sans un accord préalable écrit de MEGA International.

© MEGA International, Paris, 1996 - 2018

Tous droits réservés.

HOPEX GDPR et HOPEX sont des marques réservées de MEGA International.

Windows est une marque réservée de Microsoft.

Les autres marques citées appartiennent à leurs propriétaires respectifs.

SOMMAIRE



Introduction à HOPEX GDPR	1
A propos du RGPD	2
Qu'est-ce que le RGPD ?	2
Qu'est-ce qu'une donnée personnelle ?	2
Pré-requis à l'utilisation de HOPEX GDPR	3
Se connecter à HOPEX GDPR	4
Profils utilisés dans HOPEX GDPR	5
Résumé des profils HOPEX GDPR	5
Détail des droits des principaux profils HOPEX GDPR	6
Ressources et modèles de documents	7
Fonctionnalités communes utiles	8
<i>Afficher de manière permanente la fenêtre de propriétés</i>	8
<i>Statut de l'objet</i>	8
<i>Fonctionnalités collaboratives</i>	8
Administre HOPEX GDPR	9
Définir les éléments clés	10
Catégories de données	10
Catégories de personnes concernées	12
Activités sensibles	12
Garanties de transferts	13
Autorités de contrôle	14
Adéquation Pays	15
<i>A propos du concept d'adéquation pays</i>	15
<i>Accéder aux informations concernant l'adéquation pays</i>	15
<i>Usage des informations concernant l'adéquation pays dans HOPEX GDPR</i>	15
Mesures de sécurité	16
Définir l'organisation	18
Créer des entités juridiques et des départements	18
<i>A propos des entités et des départements</i>	18

<i>Créer une entité juridique</i>	19
<i>Créer des départements</i>	19
<i>Peupler les entités juridiques et les départements</i>	19
Définir les propriétés des entités juridiques	19
<i>Propriétés générales d'une entité</i>	20
<i>Gérer les établissements</i>	20
<i>Gérer les représentants nationaux</i>	20
<i>Gérer les accords contractuels</i>	21
<i>Gérer les utilisateurs</i>	21
Gérer les départements	22
<i>Définir les caractéristiques principales d'un département</i>	22
<i>Relier des utilisateurs à un département</i>	22
Définir les établissements	22
<i>Créer un établissement</i>	22
<i>Spécifier l'établissement « siège » de l'entité</i>	23
<i>Spécifier le pays d'une entité juridique</i>	23
Gérer les tiers	24
Visualiser l'organigramme des DPO	24
Gérer les directives RGPD de l'entreprise	24
Décrire les traitements dans HOPEX GDPR	27
Présentation des traitements	28
Créer les traitements	29
Créer des traitements à partir d'objets HOPEX	29
<i> Importer des données à partir d'HOPEX</i>	29
<i> Créer des traitements à partir de processus</i>	29
<i> Créer des sous-traitements à partir d'applications</i>	30
Créer des traitements dans HOPEX GDPR	30
Décrire les traitements	31
Accéder aux traitements	31
Décrire les traitements	31
Tableau de bord du traitement	32
Vue globale des traitements	33
<i> Informations supplémentaires à spécifier</i>	33
<i> Information calculée</i>	34
Fondement juridique du traitement	34
Détails du traitement	36
A propos des traitements	36
Analyse des risques des données à caractère personnel	37
<i> Qualifier la minimisation</i>	37
<i> Visualiser le risque calculé</i>	38
<i> Spécifier la période de conservation sur un traitement</i>	38
Gestion des droits des personnes concernées et des informations	38
<i> Spécifier les droits des personnes concernées sur un traitement</i>	39
<i> Visualiser les droits des personnes concernées sur vos traitements</i>	40
<i> Attribuer un niveau de conformité sur les droits des personnes concernées</i>	40
Transferts de données et mesures de sécurité	40
<i> Spécifier les transferts de données sur un traitement</i>	41

<i>Spécifier des mesures de sécurité sur un traitement</i>	41
<i>Attribuer un niveau de conformité à des transferts et des mesures de sécurité</i>	42
Accords contractuels et autres pièces jointes	42
Gérer les sous-traitements	43
<i>Créer un sous-traitement</i>	43
<i>Décrire un sous-traitement</i>	44
Rapports associés aux traitements	45
Accéder aux rapports associés aux traitements	45
Registres des traitements	45
<i>A propos du registre des traitements</i>	45
<i>Créer un registre des traitements</i>	45
Tableau de bord des incohérences	46
Carte des flux transfrontaliers	47
<i>Conditions préalables à l'utilisation d'une carte des flux transfrontaliers</i>	47
<i>Contenu de la carte des transferts</i>	47
<i>Informations supplémentaires sur les transferts</i>	48
Évaluer les traitements	49
Pré-requis à l'évaluation des traitements	50
Spécifier les niveaux de conformité	50
<i>Niveau de conformité Fondement juridique</i>	50
<i>Niveau de conformité Minimisation</i>	51
<i>Transferts de données et mesures de sécurité</i>	51
Visualiser le niveau de conformité initial d'un traitement	51
Réaliser une évaluation préliminaire	53
Consulter des rapports d'aide à la décision	53
<i>Accéder à votre tableau de bord</i>	53
<i>Traitements par niveau de conformité</i>	53
<i>Traitements par statut d'évaluation (DPIA)</i>	55
<i>Traitements par échelle de risque</i>	56
Réaliser une évaluation préliminaire	56
Consulter l'historique des évaluations préliminaires	57
Réaliser une analyse d'impact (DPIA)	58
A propos des DPIA	58
<i>Quand réaliser une DPIA ?</i>	58
<i>Qu'est-ce qu'une DPIA ?</i>	58
Créer une DPIA	58
<i>Démarrer une nouvelle DPIA</i>	58
<i>Réutiliser une DPIA</i>	58
<i>Modifier une DPIA</i>	59
Evaluer les risques	59
<i>Créer des risques</i>	59
<i>Propriétés des risques</i>	60
Définir des recommandations et mesures correctives	60
Valider la DPIA	61
<i>Niveau de risque final</i>	61
<i>Niveau de conformité final</i>	61
<i>Action ultérieure</i>	61

Consulter les rapports et les résultats de la DPIA	62
<i>Visualiser le tableau de bord du traitement</i>	62
<i>Registre des DPIA</i>	62
<i>Générer un document de DPIA</i>	63

Gérer les violations de données RGPD **65**

Déclarer une violation de données	65
Évaluer une violation de données	67
Planifier des mesures correctives	67
Notifier une violation de données	67
Voir le temps écoulé depuis la détection de la violation	68
Duplicer des violation de données	68

Gérer les demandes des personnes concernées **69**

Créer une demande de personne concernée	69
Détailler la demande de personne concernée	71
Décrire le périmètre de la demande de la personne concernée	71
Joindre des documents à la demande	72
Gérer les échéances des demandes	72

Démontrer la conformité **73**

Registre des DPIA	73
Rapport de cohérence	74
<i>Lancer le rapport de cohérence</i>	74
<i>Exemple de rapport de cohérence</i>	75
<i>Gérer les incohérences entre traitement et sous-traitements</i>	75
Tableau de bord des incohérences	76
Rapport de risques	77
Registre des flux de données	78
Registre des informations	79
Rapport sur les droits des personnes concernées	80
Rapport concernant les tiers	81
<i>Conditions préalables</i>	81
<i>Lancer le rapport concernant les tiers</i>	81
<i>Contenu du rapport concernant les tiers</i>	82
Registre des traitements	82
Carte des flux transfrontaliers	82

Questions fréquentes RGPD **83**

A propos des traitements	83
A propos des évaluations RGPD	83
A propos des transferts	84
A propos de l'import HOPEX GDPR	85
Divers	86

INTRODUCTION À HOPEX GDPR



HOPEX GDPR est une solution SaaS qui a pour objectif d'aider les clients à gérer leur conformité au RGPD (Règlement Général sur la Protection des Données).

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

Vous pouvez produire les documents nécessaires permettant de démontrer que vous maîtrisez la confidentialité des données à caractère personnel et que vous avez adopté les mesures de sécurité qui conviennent.

Notre méthodologie a été développée avec le groupe IMPERIALI, experts de la protection des données personnelles depuis plus de 30 ans. **HOPEX GDPR** intègre les informations réglementaires et des modèles juridiques mis à jour régulièrement pour accélérer votre mise en conformité.

A PROPOS DU RGPD

Qu'est-ce que le RGPD ?

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.

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.*

PRÉ-REQUIS À L'UTILISATION DE HOPEX GDPR

☞ Le Solution Pack que vous voulez importer est à décompresser (dossier d'installation HOPEX > Utilities > Solution Pack ; double-cliquez sur le Solution Pack pour l'extraire).

Pour importer le Solution Pack :

1. A partir d'**HOPEX Administration**, connectez-vous à l'environnement concerné.
2. Dépliez le dossier **Référentiels**.
3. Faites un clic droit sur le référentiel et sélectionnez **Gestion des objets > Importer un solution pack**.
La fenêtre Importer un solution pack apparaît.
4. Sélectionnez le Solution Pack « GDPR.exe ».
5. Cliquez sur **OK**.
La fenêtre Importation de données MEGA XML permet de visualiser la progression de l'import.
Le Solution Pack sélectionné est importé dans le référentiel.

SE CONNECTER À HOPEX GDPR

Pour vous connecter à **HOPEX GDPR** :

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. (si vous avez un mot de passe) Dans le champ **Mot de passe**, 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 GDPR", page 5](#)".

☞ *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 GDPR

Résumé des profils HOPEX GDPR

Profils	Définition
Administrateur fonctionnel RGPD	L'administrateur fonctionnel RGPD 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.
Propriétaire d'activité	Le propriétaire d'activité 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.
Propriétaire d'application	Le propriétaire d'application fournit une description des applications informatiques utilisées dans le contexte d'un traitement. Son rôle est similaire à celui du Propriétaire d'activité mais au niveau applicatif.
DPO	Le DPO joue le rôle de conseiller dans l'entreprise, de correspondant en matière de conformité au RGPD 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 le RGPD. 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. 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.
Correspondant du DPO	Le correspondant du DPO joue le même rôle que le DPO mais ses tâches se limitent à un sous-ensemble de l'organisation.
Equipe RGPD	L'équipe RGPD est constituée d'opérationnels qui suivent les instructions du DPO ou du responsable de la confidentialité. Ce profil peut être utilisé par tout membre de l'équipe responsable du niveau de conformité global de l'entreprise au RGPD.

Détail des droits des principaux profils HOPEX GDPR

Actions	Administrateur fonctionnel	Propriétaire d'activité/ Propriétaire d'application	DPO/ Equipe RGPD Responsable de la confidentialité
<p>"Définir les éléments clés"</p> <ul style="list-style-type: none"> - Catégories de données - Catégories de personnes concernées - Activités sensibles - Sécurisation des transferts - Autorités de contrôle - Adéquation Pays - Mesures de sécurité 	X		
<p>"Définir l'organisation"</p> <ul style="list-style-type: none"> - Entités juridiques - Départements - Tiers - Organigramme des DPO - Directives de l'entreprise 	X		
<p>"Décrire les traitements dans HOPEX GDPR"</p>		X	
<p>"Réaliser une évaluation préliminaire"</p> <ul style="list-style-type: none"> - Identifier le niveau de conformité - Identifier le niveau de risque 			X
<p>"Réaliser une analyse d'impact (DPIA)"</p> <ul style="list-style-type: none"> - Définir les risques - Définir les recommandations et les mesures correctives 			X
<p>"Gérer les violations de données RGPD"</p>			X
<p>"Gérer les demandes des personnes concernées"</p>			X

RESSOURCES ET MODÈLES DE DOCUMENTS

A tout moment vous pouvez accéder à une documentation de référence concernant RGPD, contenant des ressources pédagogiques et modèles de documents.

Pour accéder à la page concernant la documentation de référence :

- Dans chacune des sections du menu de navigation, sélectionnez **Ressources et Modèles**, par exemple à partir des menus :
 - **Organisation**
 - **Registre des traitements**
 - **Gestion des incidents**
 - **Rapports RGPD**

Cette documentation de référence contient :

- une documentation RGPD
 - un guide de démarrage
 - RGPD en détail
- des modèles RGPD
 - des modèles de documents contractuels
 - des modèles de documents liés à la confidentialité
 - des modèles de DPIA et instructions d'utilisation
- *Vous pouvez utiliser ces modèles de documents pour les personnaliser selon vos besoins et les utiliser comme pièces jointes comme approprié dans HOPEX GDPR.*
- Procédures SOP (Standard Operating Procedures) : Modèles de documents pour les Procédures Opérationnelles Normalisées

FONCTIONNALITÉS COMMUNES UTILES

▶ Pour plus de détails sur l'utilisation du bureau et du référentiel, voir "[Manipuler les objets du référentiel](#)".

Afficher de manière permanente la fenêtre de propriétés

Vous pouvez choisir d'afficher la fenêtre de propriétés **HOPEX** de manière permanente, de façon à visualiser rapidement les propriétés des objets.

Pour afficher de manière permanente la fenêtre de propriétés :

1. Cliquez sur le bouton **Propriétés**  en haut à droite.

La fenêtre **Propriétés** s'affiche dans la zone d'édition.

2. Sélectionnez un objet.
Ses propriétés apparaissent.

Statut de l'objet

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

Les objets de votre environnement peuvent avoir pour statut :

- **Candidat** : à valider par le DPO / l'équipe RGPD
- **Opérationnel** : a été créé et validé par le DPO / l'équipe RGPD
- **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 GDPR 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 rapide \(Web Front-End\)](#)".

- Visualiser vos activités
- Partager avec d'autres utilisateurs **HOPEX** : ajouter des balises, aimer un objet.

▶ Pour plus de détails, voir "[Communiquer dans HOPEX](#)".

ADMINISTRER HOPEX GDPR



En tant qu'**Administrateur fonctionnel RGPD**, 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 GDPR** 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.

Vous devez également définir la structure de l'organisation, en spécifiant les entités juridiques et les départements.

- ✓ "Définir les éléments clés"
- ✓ "Définir l'organisation"

DÉFINIR LES ÉLÉMENTS CLÉS

Pour visualiser et modifier les éléments clés de votre environnement :

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

Les éléments les plus importants à définir sont les suivants :

- "Catégories de données"
- "Catégories de personnes concernées".

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

- "Activités sensibles"
- "Garanties de transferts"
- "Autorités de contrôle"
- "Mesures de sécurité"
- "Adéquation Pays"

Catégories de données

Dans **HOPEX GDPR**, 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.

Pour définir les catégories de données :

1. Dans le menu de navigation, cliquez sur **Éléments clés RGPD > Catégories de données**.

2. Identifiez les catégories de données à caractère personnel les plus couramment utilisées dans vos activités métier.

	Nom de catégorie de données ↑	Période de conservation	Échelle de risque
<input type="checkbox"/>	Biométriques	1 année	Elevée
<input type="checkbox"/>	Cookies et journaux système	2 mois	Moyenne
<input type="checkbox"/>	Financières	20 ans	Elevée
<input type="checkbox"/>	Identification	1 année	Moyenne
<input type="checkbox"/>	Juridiques	10 ans	Elevée
<input type="checkbox"/>	Médicales	1 année	Elevée
<input type="checkbox"/>	Sensibles	1 année	Elevée

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 les informations suivantes sur les catégories de données :

- **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](#)".
- **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.

Catégories de personnes concernées

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 RGPD > 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.

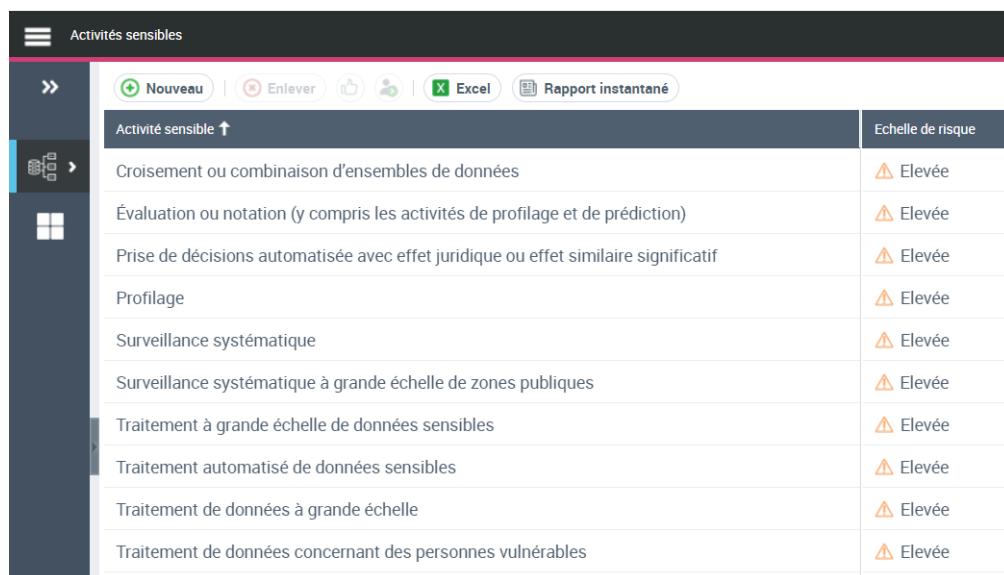
Nom de la personne concernée ↑	Echelle de risque	Description
Actionnaires	▲ Moyenne	
Agents	▲ Moyenne	
Clients	▲ Moyenne	
Conducteurs	▲ Moyenne	
Employés	▲ Moyenne	
Fournisseurs	▲ Moyenne	
Mineurs	▲ Elevée	
Visiteurs	▲ Moyenne	

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 RGPD > Activités sensibles.**



Activité sensible ↑	Echelle de risque
Croisement ou combinaison d'ensembles de données	⚠️ Elevée
Évaluation ou notation (y compris les activités de profilage et de prédition)	⚠️ Elevée
Prise de décisions automatisée avec effet juridique ou effet similaire significatif	⚠️ Elevée
Profilage	⚠️ Elevée
Surveillance systématique	⚠️ Elevée
Surveillance systématique à grande échelle de zones publiques	⚠️ Elevée
Traitemen à grande échelle de données sensibles	⚠️ Elevée
Traitemen automatisé de données sensibles	⚠️ Elevée
Traitemen de données à grande échelle	⚠️ Elevée
Traitemen de données concernant des personnes vulnérables	⚠️ Elevée

HOPEX GDPR 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** ».

Garanties de transferts

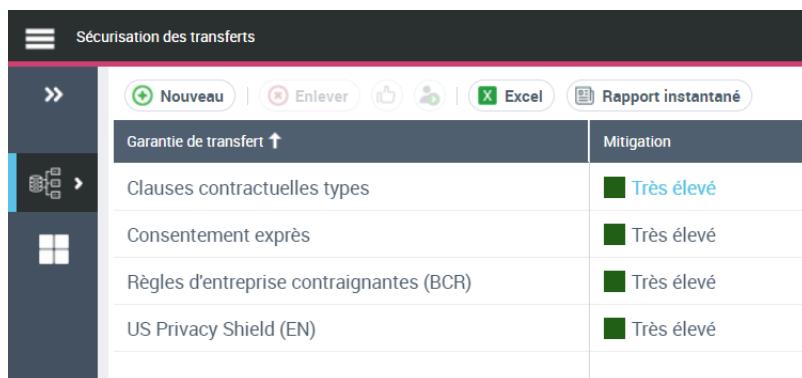
Vous devez vous assurer que les transferts de données sont légitimes et licites.

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 RGPD > Garanties de transfert.**



Garantie de transfert ↑	Mitigation
Clauses contractuelles types	■ Très élevé
Consentement exprès	■ Très élevé
Règles d'entreprise contraignantes (BCR)	■ Très élevé
US Privacy Shield (EN)	■ Très élevé

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 »).

Autorités 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 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 RGPD > 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

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 "[Garanties de transferts](#)".

Accéder aux informations concernant l'adéquation pays

Pour accéder aux informations concernant l'adéquation pays :

- » Dans le menu de navigation, cliquez sur **Éléments clés RGPD > 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 dans HOPEX GDPR

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).

Mesures de sécurité

Pour accéder aux mesures de sécurité et les définir :

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

The screenshot displays the 'Mesures de sécurité' (Security Measures) section of the RGPD navigation interface. The main area lists various security measures such as Anonymisation, Antivirus, Chiffrement, etc. A toolbar at the top provides options like 'Nouveau' (New), 'Enlever' (Delete), 'Excel', and 'Rapport instantané' (Instant Report). The left sidebar shows the navigation structure.

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 "Garanties de transferts".*

DÉFINIR L'ORGANISATION

En tant qu'administrateur fonctionnel, vous devez définir l'organisation de manière à ce que les membres de l'équipe RGPD puissent réaliser leur mission.

Pour définir l'organisation :

- » Dans le menu de navigation cliquez sur **Organisation**.

Vous pouvez créer :

- entités juridiques
 - » Voir "[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.
- départements
- Des tiers
 - » Voir "[Gérer les tiers](#)".
- Des directives d'entreprise
 - » Voir "[Gérer les directives RGPD de l'entreprise](#)".
- 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 GDPR**, 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 juridiques](#)".

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 juridiques](#)".*

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 juridiques](#)"
- "[Gérer les départements](#)"

Définir les propriétés des entités juridiques

Pour définir des informations sur une entité :

1. Dans le menu de navigation d'**HOPEX GDPR**, 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 GDPR.*

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).
☞ *Cette information dépend du pays de l'établissement principal. Si aucun établissement n'a été défini, la valeur par défaut de ce champ est « Non ».*

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 "[Gérer les tiers](#)".

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.

☞ 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 le menu de navigation cliquez sur **Organisation > Départements**.

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

Pour gérer les droits de visibilité d'un département, vous devez ajouter des utilisateurs afin que les propriétaires d'activités puissent créer des traitements.

Pour gérer les droits de visibilité du département :

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

Définir les établissements

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

Vous devez 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 "["Garanties de transferts"](#)".

- **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 **Etablissements**.
3. Cochez la case **Siège**.

Vue globale	Etablissements	Représentants nationaux	Accords contractuels	Utilisateurs
<p> Spécifier tous les établissements de cette entité juridique.</p>				
	 Nouveau  Enlever			
	Site	Pays	Siège	Garanties de transfert
	 Site Paris	 France <input type="checkbox"/>		
	 Site Moscou	 Russie <input checked="" type="checkbox"/>		

Spécifier le pays d'une entité juridique

Vous devez 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 **Etablissements**.
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"](#)"

Gérer les tiers

La gestion des tiers 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 tiers :

- » 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 juridiques".*

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 licéité du transfert de données.

Visualiser l'organigramme des DPO

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 **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 directives RGPD de l'entreprise

 *Les directives d'entreprise 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 .*

Pour gérer les directives de l'entreprise ainsi que les documents :

- » Dans le menu de navigation cliquez sur **Organisation > Directives RGPD de l'entreprise**.

Vous pouvez y joindre tout type de document important d'un point de vue du RGPD.
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
- **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
- **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](#)".

DÉCRIRE LES TRAITEMENTS



- ✓ "Présentation des traitements"
- ✓ "Conditions préalables à la création de traitements"
- ✓ "Créer les traitements"
- ✓ "Décrire les traitements"
- ✓ "Détails du traitement"
- ✓ "Gérer les sous-traitements"
- ✓ "Rapports associés aux traitements"

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

En tant que **Propriétaire d'activité (RGPD)**, vous êtes en charge de la description détaillée de 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

Votre administrateur fonctionnel 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 GDPR**.

Vous pouvez également utiliser les processus et les applications créés dans d'autres solutions **HOPEX** pour créer les traitements adéquats.

Créer des traitements à partir d'objets HOPEX

Importer des données à partir d'HOPEX

HOPEX GDPR vous permet d'importer manuellement des processus et des applications.

Pour importer des objets à partir d'**HOPEX**:

1. Dans le menu de navigation sélectionnez **Import > Import à partir d'HOPEX ou Excel**.
2. Sélectionnez le fichier à importer et cliquez sur **OK** en bas de la page (dans la partie inférieure droite).

Après l'import le propriétaire d'activité peut créer :

- des traitements à partir de processus métier/organisationnels
- des sous-traitements à partir d'applications

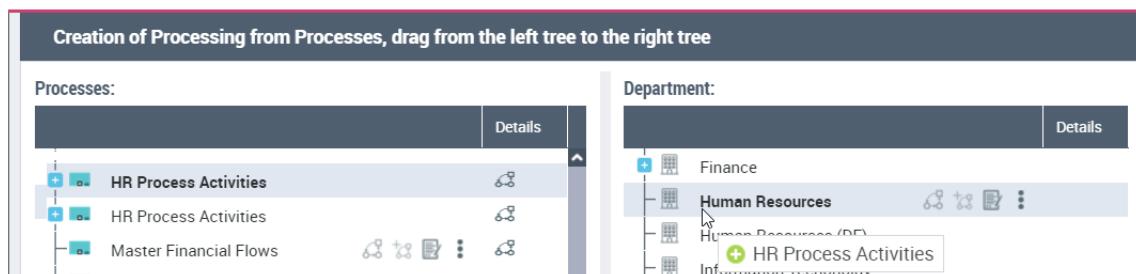
Créer des traitements à partir de processus

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 sélectionnez **Import > Créer des traitements à partir de 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.

☞ Pour créer un traitement à partir d'un sous-processus, voir les Questions Fréquentes RGPD. Voir "[A propos de l'import HOPEX GDPR](#)".

Créer des sous-traitements à partir d'applications

Une application **HOPEX** peut devenir un sous-traitement dans **HOPEX GDPR**.

☞ Pour plus de détails sur les sous-traitements, voir "[Gérer les sous-traitements](#)".

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

Pour créer des sous-traitements à partir d'applications :

1. Dans le menu de navigation sélectionnez **Import > Crée des traitements à partir d'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. Le sous-traitement est créé automatiquement sous ce traitement.

☞ Le bouton **Créer un nouveau traitement** vous permet également de créer directement le sous-traitement voulu sous le département concerné.

Créer des traitements dans HOPEX GDPR

Pour créer un traitement directement dans **HOPEX GDPR** :

1. Dans le menu de navigation sélectionnez **Registre des traitements**.
2. Cliquez sur **Nouveau**.

Si besoin vous pouvez créer des sous-traitements. Dans ce cas, il est conseillé de décrire dans un premier temps le traitement général et de créer par la suite des sous-traitements lorsque des différences existent sur certaines parties du traitement.

☞ Pour plus de détails, voir "[Gérer les sous-traitements](#)".

DÉCRIRE LES TRAITEMENTS

En tant que propriétaire d'activité, vous devez décrire le détail de traitements.

☞ Pour plus de détails sur la création de traitements, voir "Créer les traitements".

Accéder aux traitements

Pour accéder aux traitements dans **HOPEX GDPR** :

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

Décrire les traitements

☞ Voir "Accéder aux traitements".

En tant que propriétaire d'activité, vous pouvez décrire un traitement en utilisant 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".

The screenshot shows the 'Treatment Details' page for a treatment named 'Financial Reporting'. At the top, there is a navigation bar with tabs: 'Statut: * Candidat', 'Vue globale' (which is highlighted with a red box), 'Fondement juridique', 'Détails', 'Evaluation préliminaire', and 'DPIA'. Below the tabs, there are four status indicators: 'Aucun' (Risk level), 'Aucun' (Conformity level), '0' (Inconsistency), and 'Aucun' (Evaluation freshness). At the bottom, there are input fields for 'Traitement: * Financial Reporting', 'Entité juridique: XCorp HQ', 'ID: P.375', 'Département: * Finance', and a dropdown menu for 'DPIA'.

☞ Les onglets **Evaluation préliminaire** et **DPIA** sont réservés à l'équipe RGPD. Pour plus de détails, voir "Évaluer les traitements".

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 RGPD 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**
- **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 d'activité**
 -  *Le propriétaire d'activité (RGPD) fournit une description détaillée du traitement. Il ne participe pas à l'évaluation du traitement.*
- **Détails** : 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 "Activités sensibles".*

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 correspondant DPO est défini au niveau du département.*
- **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*

I'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.

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
- niveau de conformité

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

Date de création	Date d'évaluation	Statut d'évaluation	Echelle de risque	Niveau de conformité
26/06/2018	22/08/2018	Réalisé	⚠ Moyenne	☑ Quasi-conforme
16/08/2018				

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.

Six fondements juridiques existent pour le traitement. Ils sont exposés dans l'article 6 du RGPD. 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 RGPD peut évaluer par la suite le **Fondement juridique** à partir des options sélectionnées précédemment par le propriétaire d'activité.

DÉTAILS DU TRAITEMENT

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

A propos des traitements

Tout traitement doit être décrit à un premier niveau général.

Il peut être nécessaire de créer des sous-traitements 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 sous-traitements et saisissez les informations qui diffèrent du traitement général.

☞ Pour plus de détails, voir "[Créer un sous-traitement](#)".

Vue globale	Fondement juridique	Détails	Evaluation préliminaire	DPIA
<i>i Spécifier les détails du traitement tels que les catégories de données et de personnes concernées, les droits d'accès, la durée de conservation des notifications et du consentement, les flux de données et les mesures de sécurité.</i>				
Vue de détails		Vue de l'évaluation		
				
Elément de traitement ↑	Type	Organisation	Rôle de protection des données	
Traitement général				Responsable de traitement
Sous-traitement1	Sous-traitant	XCorp Italy (...)	Sous-traitant	
Sous-traitement2	Sous-traitant	XCorp Germa...	Co-responsable du traite...	

Pour le traitement général vous pouvez saisir les informations suivantes.

- "Analyse des risques des données à caractère personnel"
- "Gestion des droits des personnes concernées et des informations"
- "Transferts de données et mesures de sécurité"
- "Accords contractuels et autres pièces jointes"

Analyse des risques des données à caractère personnel

Pour créer un risque associé à des données dans **HOPEX GDPR**:

1. Ouvrez les propriétés du traitement.
2. Sous la section **Détails > Analyse de risque des données personnelles**, cliquez sur **Nouveau**.

The screenshot shows a dialog box titled "Nouveau risque concernant les données personnelles". It contains the following fields:

- Catégories de données:** Identification (selected), Financières
- Personnes concernées:** Clients
- Minimisation:** Elevé
- Période de conservation:** 2, Unité: Jours, Période illimitée
- Commentaire:** A rich text editor with a toolbar showing icons for bold, italic, underline, superscript, subscript, and alignment.

Vous pouvez spécifier les informations suivantes :

- **Catégories de données**
- **Personnes concernées**
- **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.

Selon l'article 5 du règlement, 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

Par la suite, l'équipe RGPD peut définir un niveau de conformité dans la section Analyse de risque des données personnelles, basé sur les informations saisies par le propriétaire d'activité :

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

Visualiser le risque calculé

A la création d'un risque sur des données personnelles, le niveau de **Risque** est automatiquement calculé à partir de l'échelle de risque la plus haute spécifiée par l'administrateur fonctionnel dans la section **Eléments clés** (pour les catégories de données et les catégories de personnes concernées).

☞ Pour plus d'informations sur l'échelle de risque initiale définie par l'administrateur, voir "[Catégories de données](#)" et "[Catégories de personnes concernées](#)".

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 rétention visée correspond à la période de rétention 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 "Registre des 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.*

— Gestion des droits des personnes concernées & des informations de Traitement général

 Spécifier les droits des personnes concernées, et le cas échéant, joindre tout document utile dans la section prévue à cet effet (par exemple, une procédure d'exploitation spécifique pour la gestion des demandes des personnes concernées s'appliquant à ce traitement en particulier).

<input type="checkbox"/> Accès <input type="checkbox"/> Opposition <input type="checkbox"/> Limitation <input type="checkbox"/> Droit à l'oubli	<input type="checkbox"/> Suppression <input type="checkbox"/> Portabilité <input type="checkbox"/> Rectification
Information: <div style="display: flex; justify-content: space-between;"> <input type="radio"/> Oui, par écrit <input type="radio"/> Oui, oralement </div> <div style="display: flex; justify-content: space-between;"> <input type="radio"/> Non <input type="radio"/> Non obligatoire </div> <div style="display: flex; justify-content: space-between;"> <input type="radio"/> Ne sais pas </div>	
Consentement: <div style="display: flex; justify-content: space-around;"> <input type="radio"/> Oui <input type="radio"/> Non </div>	
Niveau de conformité Gestion des droits des personnes concernées et des informations: 	

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 d'activité ou d'application, vous pouvez visualiser sur les traitements dont vous êtes responsable les droits des personnes concernées.

HOPEX GDPR fournit un rapport pour cela.

Pour avoir une vue générale des droits des personnes concernées :

- Dans le bureau du propriétaire d'activité, cliquez sur **Rapports RGPD > Droits des personnes concernées**.

Attribuer un niveau de conformité sur les droits des personnes concernées

Par la suite, dans cette section, l'équipe RGPD 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 et mesures de sécurité

Cette section vous permet de créer les transferts de données et les mesures de sécurité 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 "["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 "["Catégories de personnes concernées"](#) 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 "["Garanties de transferts"](#).*
- si les données sont externalisées
- si les données sont vendues/achetées

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. Défilez 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 "[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 à des transferts et des mesures de sécurité

Par la suite, dans cette section, l'équipe RGPD 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, défilez jusqu'à la section des transferts et des mesures de sécurité.
2. Dans le champ **Niveau de conformité Transferts de données & Mesures de sécurité**, sélectionnez une valeur dans le menu déroulant.

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 GDPR 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 RGPD** : oui/non
 - **Sous-traitance**: indiquez si le traitement peut faire appel à des sous-traitants.

GÉRER LES SOUS-TRAITEMENTS

Si vous avez besoin d'une vue globale, vous pouvez traiter uniquement le traitement général (ce qui signifie que des sous-traitements ne sont pas nécessaires).

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 sous-traitement afin de le décrire plus finement.

Les informations peuvent être saisies à tous les niveaux de traitement et de sous-traitement. Des incohérences peuvent résulter de cette double saisie.

Lorsque des incohérences sont détectées, un avertissement apparaît et indique le nombre d'incohérences trouvées. Pour plus de détails sur les incohérences, voir "[Tableau de bord des incohérences](#)".

Créer un sous-traitement

Pour créer un sous-traitement :

1. Sélectionnez un traitement pour ouvrir sa page de propriétés.
2. Sélectionnez l'onglet **Détails**.
3. Dans la section **Vue de détails**, cliquez sur **Nouveau sous-traitement**.



4. Sélectionnez le type de sous-traitement.

- Organisation
- Sous-traitant
- Application

Vous pouvez fournir des informations sur le rôle de protection des données du fournisseur d'application ou du sous-traitant.

Décrire un sous-traitement

Pour décrire un sous-traitement :

1. Sélectionnez le sous-traitement créé.

Notez que la page de propriétés s'applique au sous-traitement.

The screenshot shows a software interface titled "Payroll Management (EN)". At the top, there is a status indicator "Statut: * Candidat" and a navigation bar with tabs: "Vue globale", "Fondement juridique", "Détails" (which is highlighted in blue), "Evaluation préliminaire", and "DPIA". Below the tabs, there is a note: "Spécifier les détails du traitement tels que les catégories de données et de personnes concernées, les droits des personnes concernées, la gestion des notifications et du consentement, les flux de données et". Under the "Détails" tab, there are two sub-tabs: "Vue de détails" (selected) and "Vue de l'évaluation". Below these are buttons for "Nouveau sous-traitement" (New subcontractor), "Supprimer" (Delete), and "Excel". A table follows with columns: "Elément de traitement ↑", "Type", "Organisation", and "Rôle de protection des d...". The first row shows "Payroll Management (...)" under "Traitement". The second row shows "HR Application" under "Sous-traitant".

Les informations saisies sur le sous-traitement doivent être cohérentes avec les informations saisies dans le traitement principal.

☞ Si des incohérences apparaissent, elles sont mentionnées dans le tableau de bord de l'onglet **Vue globale**. Pour plus d'informations sur les incohérences, voir "[Incohérences](#)".

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 rapport disponible dans le menu déroulant du bouton **Rapport**.

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 GDPR. 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 **Registre des 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 et mesures de sécurité](#)".
 - Mesures de sécurité
 - ▶ Voir "[Transferts de données et mesures de sécurité](#)".
 - Éléments de sous-traitement
 - ▶ Voir "[Vue globale des traitements](#)".
 - Pièces jointes
 - ▶ Voir "[Accords contractuels et autres pièces jointes](#)".

Tableau de bord des incohérences

▶ Voir "[Accéder aux rapports associés aux traitements](#)".

Certains rapports peuvent vous aider à suivre les incohérences entre les traitements et les sous-traitements.

Pour la description de ces rapports, voir :

- "[Rapport de cohérence](#)"
 - ▶ Le rapport de cohérence vous permet également de supprimer/d'ajouter des droits et des transferts.
- "[Tableau de bord des incohérences](#)"

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

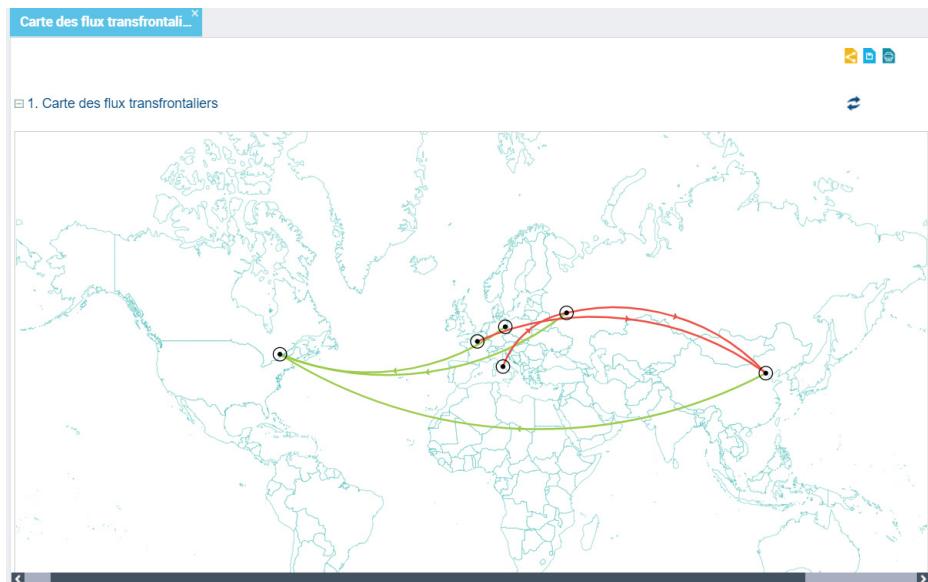
Assurez-vous que :

- 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 "[Garanties de transferts](#)".



☞ 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](#)".

ÉVALUER LES TRAITEMENTS



L'équipe RGPD ou le DPO évaluent les traitements après que le propriétaire d'activité a décrit ces mêmes traitements.

☞ Pour plus de détails sur la description des traitements, voir "[Décrire les traitements dans HOPEX GDPR](#)"

Les onglets d'intérêt pour l'équipe RGPD qui évalue les traitements sont les suivants :

The screenshot shows a software interface for managing data processing activities. At the top, it says "Acheter des Biens et Services (FR)". Below that is a status dropdown labeled "Statut: * Candidat". A navigation bar contains five tabs: "Vue globale" (highlighted in blue), "Fondement juridique", "Détails", "Evaluation préliminaire" (highlighted with a red box), and "DPIA".

☞ Pour des questions fréquentes concernant l'évaluation des traitements, voir "[A propos des évaluations RGPD](#)".

PRÉ-REQUIS À L'ÉVALUATION DES TRAITEMENTS

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

- Les propriétaires d'activités ont décrit de manière appropriée les traitements
 - ☞ Pour plus de détails, voir "[Décrire les traitements dans HOPEX GDPR](#)".
- Vous avez spécifié les niveaux de conformité en vous basant sur les informations saisies par les propriétaires d'activités.
 - ☞ Voir "[Spécifier les niveaux de conformité](#)".

Spécifier les niveaux de conformité

L'équipe RGPD/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 d'activité 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.

Vue globale	Fondement juridique	Détails	Evaluation préliminaire	DPIA
<p>Spécifiez le fondement juridique du traitement et joindre tout document pertinent. Ceci constitue le motif juridique démontrant la légitimité du traitement.</p> <p><input type="checkbox"/> Obligation contractuelle <input type="checkbox"/> Application du droit <input type="checkbox"/> Intérêt vital <input type="checkbox"/> Intérêt légitime <input type="checkbox"/> Intérêt public <input type="checkbox"/> Consentement exprès</p> <p>Description: <input type="text"/></p> <p>Niveau de conformité Fondement juridique: <input type="button" value="▼"/></p>				

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 "Analyse des risques des données à caractère personnel".](#)

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 et mesures de sécurité".](#)

Visualiser le niveau de conformité initial d'un traitement

Il est utile au DPO ou à l'équipe RGPD 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 **Evaluation préliminaire**.

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

Acheter des Biens et Services

Statut: *  Production

Vue globale | Fondement juridique | Détails | **Evaluation préliminaire** | DPIA

i Effectuer une évaluation globale du traitement sur la base des informations fournies dans les sections précédentes. L'objectif de l'évaluation préliminaire est d'identifier les traitements qui se caractérisent par un niveau de risque élevé et un faible niveau de conformité, et qui nécessitent une DPIA ou des ajustements.

 Quasi-conforme Fondement juridique	 Quasi-conforme Minimisation des données
 Moyen Gestion des droits des personnes concernées et des informations	 Non conforme Transferts de données & Mesures de sécurité

- Fondement juridique (score défini dans l'onglet Fondement juridique)
➡ Voir "[Fondement juridique du traitement](#)".
- Minimisation des données (score défini dans l'onglet Détails).
➡ Voir "[Analyse des risques des données à caractère personnel](#)".
- 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](#)".
- Gestion des transferts et des mesures de sécurité (score défini dans l'onglet Détails)
➡ Voir "[Transferts de données et 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 d'activité 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 GDPR** 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 doit être amélioré.

Votre tableau de bord contient trois 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 diagramme, 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.

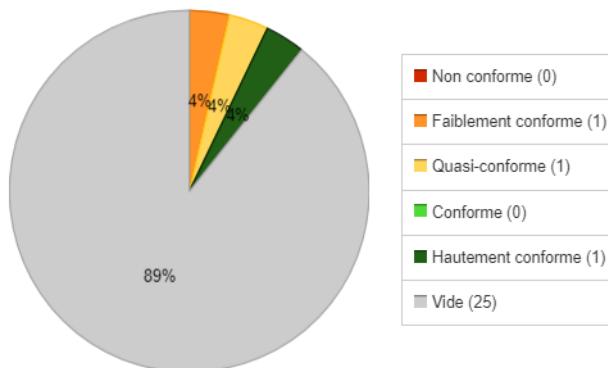
☞ *Les informations affichées proviennent des évaluations préliminaires ou des DPIA (le résultat du plus récent des deux types d'évaluation est pris en compte).*

RGPD - Traitements par niveau de conformité

⤵ ⌧ ⌨ 〈

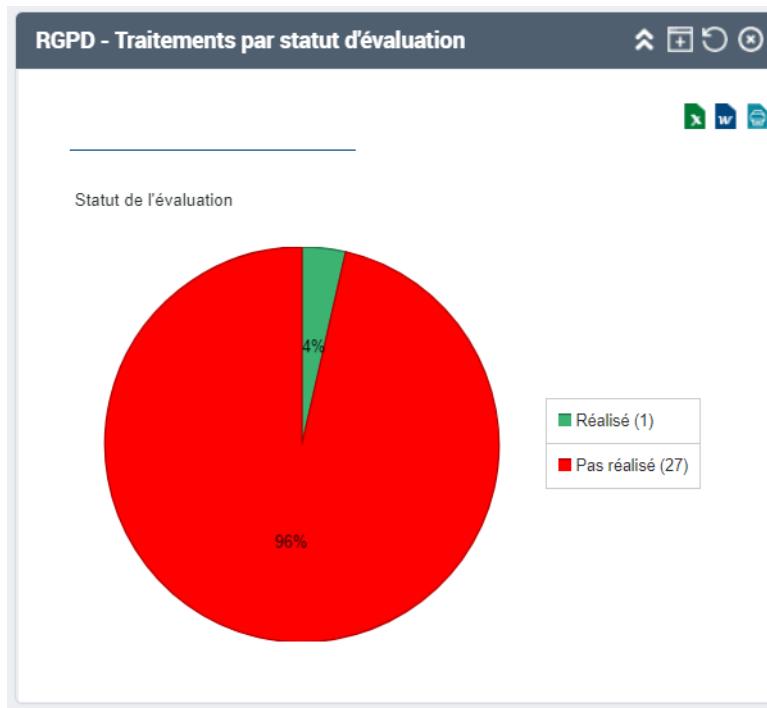
x w 📈

Niveau de conformité



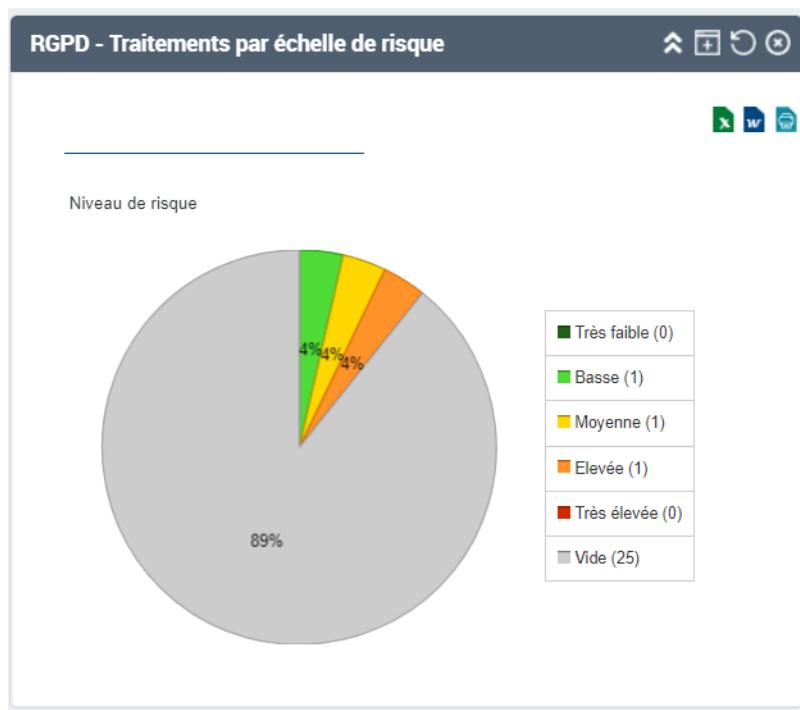
Traitements par statut d'évaluation (DPIA)

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 **Evaluation 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**.

► Il est important de saisir un commentaire de manière à justifier votre choix.

3. Indiquez les **Actions ultérieures** à réaliser :
 - Rien
 - Arrêter le traitement
 - Notifier l'autorité de contrôle
 - Autres
4. Une fois que vous avez saisi toutes les informations nécessaires, cliquez sur **Enregistrer l'évaluation préliminaire**.

— Validation

Niveau de conformité final:	<input checked="" type="radio"/> Faiblement conforme	Commentaire:	<input type="text"/>
Niveau de risque final:	<input checked="" type="radio"/> Moyenne	Commentaire:	<input type="text"/>
Actions ultérieures:	Lancer la DPIA	Commentaire:	<input type="text"/>
Nom de l'évaluation préliminaire:		<input type="text" value="EvaluationPréliminaireMonTraitement"/> Enregistrer l'évalu...	

☞ 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 **Evaluation préliminaire** de la page de propriété du traitement, dépliez la section **Historique des évaluations préliminaires**.

— Historique des évaluations préliminaires

Nom Local ↑	Date d'achèvement	Niveau de conformité	Actions ultérieures	Niveau de risque final
EvalAchatBiensServices	23/08/2018	<input checked="" type="radio"/> Faiblement conforme	Lancer la DPIA	<input checked="" type="radio"/> Elevé

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 RGPD) 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 "[Evaluer les risques](#)".
- Les actions correctives qui permettent d'assurer que le traitement est sous contrôle.

☞ Pour plus de détails, voir "[Définir des recommandations et mesures correctives](#)".

Créer une DPIA

Démarrer une nouvelle DPIA

Pour démarrer une 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 de cette manière 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. Dans la page de création d'une DPIA, cliquez sur **Importer une DPIA**.
4. 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 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 "[Démarrer une nouvelle DPIA](#)".*

Evaluer les risques

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

Créer des risques

Pour définir des risques dans **HOPEX GDPR** :

1. Dans la fenêtre de la DPIA, dépliez la section **Risques pour le respect de la vie privée**.
2. Dans les différents onglets correspondant aux différents types de risque, cliquez sur **Nouveau** pour créer un risque.

Il est possible de distinguer les types de risque suivants :

- Accès illégitime
- Perte de données
- Intégrité des données
- Non disponibilité des données
- Traitement illicite

Propriétés des risques

Probabilité

- Rare
- Possible
- Vraisemblable
- Certaine

Sévérité du risque

- Très faible
- Basse
- Moyenne
- Elevée

Impact sur les personnes concernées

Dans ce champ vous pouvez saisir une description des impacts sur les personnes concernées si le risque survient.

Causes du risque

Dans ce champ vous pouvez saisir les causes les plus courantes qui peuvent engendrer ce risque.

Mesures de sécurité

Dans ce champ vous pouvez sélectionner un groupe des mesures de sécurité prises pour traiter ce risque.

☞ Les mesures de sécurité sont des données de référence définies par l'administrateur fonctionnel. Pour plus de détails, voir "[Mesures de sécurité](#)".

- Technique
- Organisationnel
- Certification

Pour plus d'informations sur ces mesures de sécurité, voir "[Spécifier des mesures de sécurité sur un traitement](#)".

Définir des recommandations et mesures correctives

La seconde étape lors de la réalisation de la DPIA consiste à définir des recommandations et mesures correctives.

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

☞ Pour plus de détails, voir "[Evaluer les risques](#)".

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

1. Dans la fenêtre de la DPIA, dépliez la section **Recommandations et actions correctives**.

☞ Pour accéder à la fenêtre de la DPIA, voir "[Créer une DPIA](#)".

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.

Valider la DPIA

Dans cette section le DPO doit 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

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

Une fois la DPIA réalisée, 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 dernière échelle 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.

Incohérences

Des incohérences peuvent apparaître lorsque des sous-traitements ont été créés.

- ☞ Pour plus de détails sur les sous-traitements, voir "[Gérer les sous-traitements](#)".

Lorsque certaines informations saisies au niveau du sous-traitement diffèrent de celles saisies au niveau du traitement général, le nombre d'incohérences détectées apparaît.

Pour corriger les incohérences :

- Copiez manuellement les informations saisies au niveau du sous-traitement et reportez-les au niveau du traitement général.

- ☞ Les incohérences peuvent concerner les personnes concernées, les catégories de données ainsi que les transferts de données.

Certains rapports peuvent vous aider à détecter les incohérences. Pour plus de détails, voir "[Rapport de cohérence](#)" et "[Tableau de bord des incohérences](#)".

Fraîcheur de l'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 DIPA et cliquez sur **Document DPIA**.

Historique des DPIA				
Document DPIA	Excel	Rapport instantané	Afficher les filtres	
Nom Local ↑	Date d'achèvement	Niveau de conformité	Actions ultérieures	Niveau de risque final
DPIA concernant Accidents ...	22/08/2018	Quasi-conforme	Notifier l'autorité de c...	Moyen

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 RGPD



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

HOPEX GDPR 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 GDPR**.

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 **Violation des données personnelles** et cliquez sur **Nouveau**.

The dialog box is titled "Nouvelle violation". It contains the following fields:

- Statut: * (Status): Soumis (Submitted)
- Description de la violation: * (Description of the violation): Violation de données RGPD-1
- Date de détection: (Detection date): Calendar icon
- Dénonciateur: (Denominator): Text input field
- Date de la violation: (Date of the violation): Calendar icon
- Nombre de personnes impactées: (Number of people impacted): Dropdown menu
- Source: (Source): Dropdown menu
- Catégories de données impliquées: (Categories of data involved): Dropdown menu
- Personnes concernées impactées: (Affected individuals): Dropdown menu

At the bottom right are "OK" and "Annuler" buttons.

2. Décrivez la violation de données :

- **Description de la violation**
- **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 "[Catégories de données](#)".

- **Personnes concernées impactées**

☞ Pour plus de détails, voir "[Catégories de personnes concernées](#)".

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

- l'évaluation de la violation : voir "[Évaluer une violation de données](#)"
- la notification de la violation : voir "[Notifier une violation de données](#)"



Évaluer une violation de données

Pour évaluer une violation de données :

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

Ici vous pouvez :

- décrire les conséquences de la violation
- créer des mesures correctives

☞ 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 **Violation des données personnelles**.
 2. Sélectionnez une violation de données et dans sa page de propriétés, sélectionnez l'onglet **Evaluation 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 **Violation des données personnelles**.
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 avez 72 heures pour agir et la signaler aux autorités ou personnes concernées.

HOPEX GDPR 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 **Violation des données personnelles**.
2. Dans la liste des violations, sélectionnez celle qui vous intéresse et consultez la colonne **Temps écoulé (heures) depuis la découverte de la violation**.

Duplicer des violation de données

Vous pouvez dupliquer des violations de données.

Pour ce faire :

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

1. Dans le menu de navigation, cliquez sur **Violation des données personnelles**.
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**.

GÉRER LES DEMANDES DES PERSONNES CONCERNÉES



La législation exige de conserver toutes les demandes qui émanent des personnes concernées. HOPEX GDPR 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 **Gestion des personnes concernées > Demandes des personnes concernées**.
2. Cliquez sur **Nouveau**.

Vous pouvez fournir les informations suivantes :

- **Statut de la demande**
 - Demande en attente
 - Nouvelle
 - Assignnée
 - 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.

► Le droit d'accès est un principe clé du RGPD.

- 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 **Gestion des 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 **Gestion des 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 **Gestion des personnes concernées > Demandes des personnes concernées**.
2. Dans les colonnes disponibles sur la demande, cochez la case **Prolongation de la date limite**.

DÉMONTRER LA CONFORMITÉ



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

Pour accéder aux rapports RGPD :

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

Registre des DPIA

Pour lancer ce rapport :

- » Dans le menu de navigation, sélectionnez **Rapports RGPD > 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 cohérence

Ce rapport affiche les sous-traitements qui ne sont pas cohérents avec le traitement général.

▶ Pour plus de détails sur les sous-traitements et le traitement général, voir :

- "Décrire les traitements dans HOPEX GDPR"
- "Gérer les sous-traitements"

Il détecte les éléments qui ont été ajoutés au sous-traitement et qui ne sont pas dans le traitement général.

Il analyse les données suivantes :

- les catégories de données
- les personnes concernées
- les transferts de données
- les droits des personnes concernées

Lancer le rapport de cohérence

Pour lancer ce rapport :

- » Dans le menu de navigation, sélectionnez **Rapports RGPD > Rapport de cohérence**.

▶ Vous pouvez également accéder à ce rapport à partir de la liste des traitements (dans le menu de navigation, sélectionnez **Registre des traitements**).

Exemple de rapport de cohérence

1. Rapport de cohérence

Cohérence des catégories de données :

Nom du traitement	Nom du sous-traitement	Data Category
Traitement général	Sous-traitement2	Biométriques
		Médicales

Cohérence des personnes concernées :

Nom du traitement	Nom du sous-traitement	Catégorie de personnes concernées
Traitement général	Sous-traitement2	Conducteurs

Cohérence des droits :

Nom du traitement	Nom du sous-traitement	Droits	Action
Traitement général	Sous-traitement1	Rectification	Ajouter au traitement Enlever du sous-traitement
	Sous-traitement2	Rectification	Ajouter au traitement Enlever du sous-traitement

Cohérence des transferts de données :

Nom du traitement	Nom du sous-traitement	Transfert de données	Action
Traitement général	Sous-traitement1	Transfert de données-12	Ajouter au traitement Enlever du sous-traitement

Gérer les incohérences entre traitement et sous-traitements

Le rapport de cohérence vous permet de résoudre les incohérences détectées entre un traitement et ses sous-traitements.

Incohérences sur les droits des personnes concernées et les transferts de données

Pour ajouter un droit d'une personne concernée ou un transfert de données au traitement général :

- » Dans la colonne **Action** correspondante du rapport, sélectionnez **Ajouter au traitement**.

Pour supprimer un droit d'une personne concernée ou un transfert de données au traitement général :

- » Dans la colonne **Action** correspondante du rapport, sélectionnez **Enlever du traitement**.

Cohérence des droits :

Nom du traitement	Nom du sous-traitement	Droits	Action
Traitement général	Sous-traitement1	Rectification	Ajouter au traitement Enlever du sous-traitement
	Sous-traitement2	Rectification	Ajouter au traitement Enlever du sous-traitement

Incohérences sur les personnes concernées et les catégories de données

Les incohérences relatives aux personnes concernées et aux catégories de données sont également listés dans le rapport.

Cependant, vous devez les corriger manuellement. Pour ce faire :

1. Ouvrez la page de propriétés du traitement.
2. Sous l'onglet **Détails**, sélectionnez le sous-traitement indiqué par le rapport.
3. Comparez les personnes concernées et les catégories de données définies au niveau du traitement et du sous-traitement.
4. Ajoutez ou enlevez manuellement les éléments concernés.

Cohérence des catégories de données :

Nom du traitement	Nom du sous-traitement	Data Category
Traitement général	Sous-traitement2	Biométriques Médicales

Exemples de catégories qui nécessitent d'être vérifiées sur le traitement/sous-traitement.

Tableau de bord des incohérences

Le tableau de bord des incohérences analyse les incohérences entre le traitement principal et les sous-traitements en termes de :

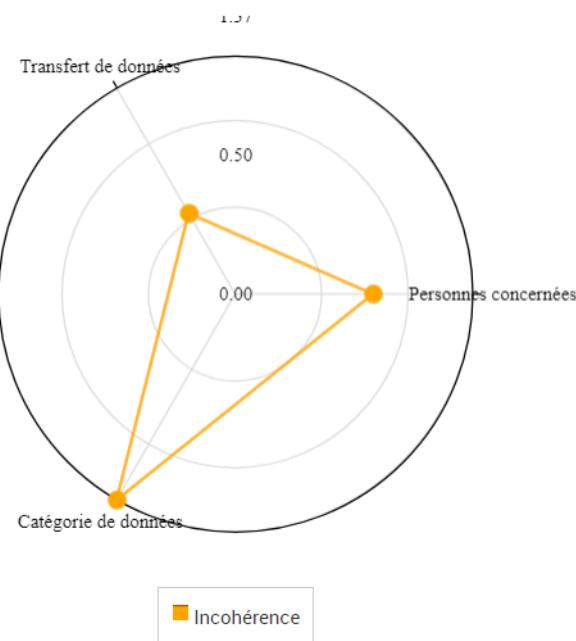
- transferts de données
- catégories de personnes concernées
- catégories de personnes concernées

Le but du rapport est de vous donner une idée générale du type de données à étudier dans les traitements afin de détecter les incohérences.

Pour lancer le tableau de bord des incohérences :

- Dans le menu de navigation, sélectionnez **Rapports RGPD > Tableau de bord des incohérences.**

L'exemple de rapport ci-dessous indique que vous devez chercher les incohérences sous les Catégories de données.



➤ Notez que les incohérences sur les catégories de personnes concernées posent un problème et qu'elles doivent être traitées.

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 RGPD > Rapport de risques.**

Le rapport contient deux tableaux :

- un pour les catégories de données
☞ Pour plus de détails, voir "[Catégories de données](#)".
- un autre pour les catégories de personnes concernées
☞ Pour plus de détails, voir "[Catégories de personnes concernées](#)".

□ 1. Rapport des catégories de données



Data Category	Niveau de risques des données par défaut	Traitement	Evaluation préliminaire	Niveau de risque	Niveau de conformité	DPIA	Niveau de risque final	Niveau de conformité final
Biométriques	⚠️ Elevée	Accidents and diseases management (EN)	Yes (23/08/2018)	⚠️ Elevée	🟢 Hautelement conforme	Yes (23/08/2018)	⚠️ Elevée	🟡 Quasi-conforme
Cookies et journaux système	⚠️ Moyenne	Accidents and diseases management (EN)	No	⚠️ Elevée	🟢 Hautelement conforme	No	⚠️ Elevée	🟡 Quasi-conforme
Financières	⚠️ Elevée	Accidents and diseases management (EN)	Yes (23/08/2018)	⚠️ Elevée	🟢 Hautelement conforme	No	⚠️ Elevée	🟡 Quasi-conforme
		Design of Organization Structure and Pay Structure-MA (EN)	No			No		
		Traitement général	Yes (23/08/2018)	⚠️ Basse	🟡 Quasi-conforme	Yes (23/08/2018)	⚠️ Très faible	🟡 Quasi-conforme
		Business Process-1 (EN)	No			No		
		Acheter des Biens et Services	Yes (23/08/2018)	⚠️ Elevée	🟡 Faiblement conforme	Yes (23/08/2018)	⚠️ Moyenne	🟡 Faiblement conforme

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.

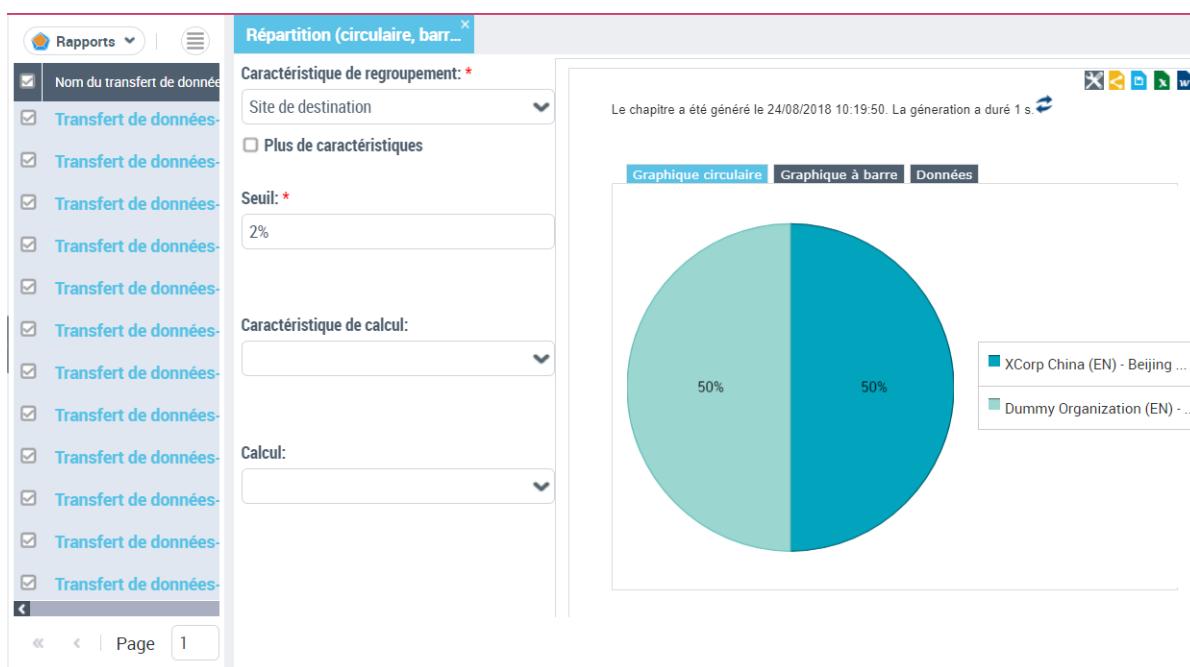
☞ Vous pouvez générer le rapport au format MS Word en cliquant sur l'icône correspondante dans le rapport.

Registre des flux de données

Le rapport contient une liste des transferts de données personnelles existants, à la fois vers les filiales et les tierces parties.

Pour lancer un rapport instantané sur des flux de données :

1. Dans le menu de navigation, sélectionnez **Rapports RGPD > Registre des flux de données**.
2. Sélectionnez les transferts de données que vous voulez inclure dans le rapport.
3. Cliquez sur le bouton **Rapport Instantané**.



Exemple de rapport qui illustre des transferts de données

☞ Pour plus de détails, voir "[Gérer des rapports instantanés](#)".

Pour construire la carte qui illustre des transferts de données :

- » Sélectionnez les transferts de données et cliquez sur **Rapports > Carte des flux transfrontaliers**.

☞ Pour plus de détails, voir "[Carte des flux transfrontaliers](#)".

Registre des informations

Ce rapport contient toutes les informations utilisées par l'entreprise dans les différents traitements.

Pour lancer ce rapport :

- » Dans le menu de navigation, sélectionnez **Rapports RGPD > Registre des informations**.

La liste indique :

- le nom des traitements
- si une information a été fournie et comment (oralement ou par écrit)

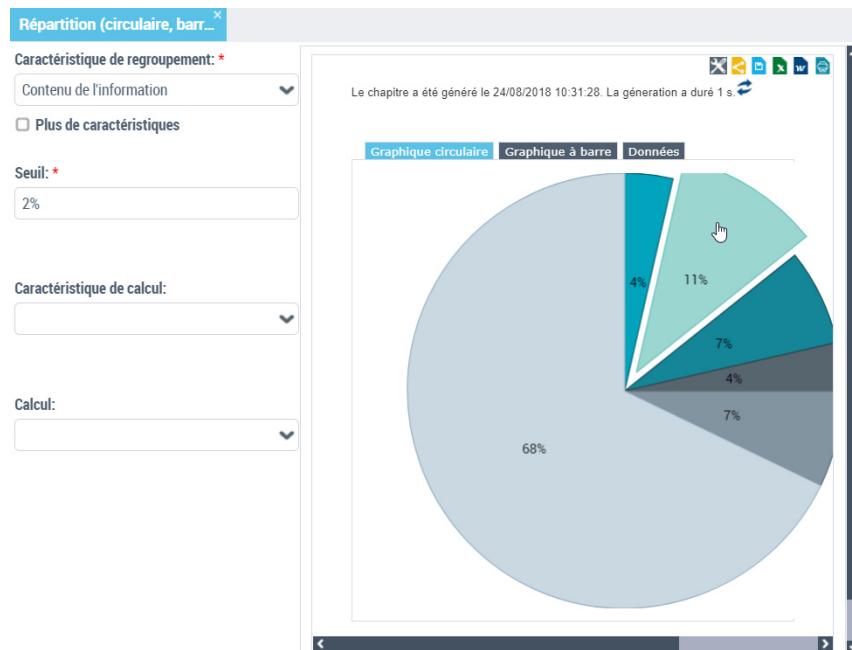
L'information est retrouvée à partir de la section **Gestion des droits des personnes concernées et des informations** d'un traitement. Vous pouvez

modifier cette information dans la page des propriétés d'un traitement, en éditant la section en question.

➤ Pour plus de détails, voir "[Gestion des droits des personnes concernées et des informations](#)".

Pour lancer un rapport graphique sur la gestion de l'information :

1. Sélectionnez les traitements qui vous intéressent et cliquez sur **Rapport instantané**.
2. Sélectionnez le type de présentation approprié, par exemple « répartition » (circulaire, barres).



Rapport sur les droits des personnes concernées

Pour afficher un rapport sur les droits des personnes concernées :

- Dans le menu de navigation, sélectionnez **Rapports RGPD > Droit 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	O
Accidents and diseases management (EN)	■	■	■	■
Achats	■	■	■	■
Acheter des Biens et Services	■	■	■	■

➤ 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 les traitements à afficher dans le rapport, vous devez avoir créé un sous-traitement de type « Sous-traitant ».

Elément de traitement ↑	Type	Organisation	Rôle de protection des données
Traitement général			Responsable de traitement
Sous-traitement1	Sous-traitant	XCorp Italy (EN)	Co-responsable du traitement

Lancer le rapport concernant les tiers

Pour lancer le rapport concernant les tiers :

- Dans le menu de navigation, sélectionnez **Rapports RGPD > 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. Tierces parties actives

Nom du tiers	Traitement	Risque brut	Niveau de conformité	Date de dernière évaluation
Tierce-partie1	Traitement général	High	Almost Compliant	24/08/2018
Tierce-partie2	Traitement général	High	Almost Compliant	24/08/2018

□ 2. Tierces parties obsolètes

Nom du tiers	Traitement	Risque brut	Niveau de conformité	Date de dernière évaluation

Le rapport distingue :

- les tierces parties actives
- Les tierces parties obsolètes

Registre des traitements

HOPEX GDPR 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

Voir "[Rapports associés aux traitements](#)" pour la description des rapports disponibles sur les traitements.

QUESTIONS FRÉQUENTES RGPD



A propos des traitements

☞ Pour des informations générales sur les traitements, voir "[Décrire les traitements dans HOPEX GDPR](#)".

Pourquoi ne puis-je pas créer de traitement ?

L'administrateur fonctionnel 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](#)".

A propos des évaluations RGPD

☞ 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](#)".
 - ➡ Cette information s'applique 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 GDPR** :

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 RGPD > 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](#)".

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 GDPR** vous permet d'afficher une carte des flux transfrontaliers.

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 HOPEX GDPR

Pour plus de détails, voir "[Créer des traitements à partir d'objets HOPEX](#)".

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 **Registre des 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 GDPR.*

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 juridiques](#)". 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 l'administrateur fonctionnel RGPD peut créer des entités juridiques et des départements.

Assurez-vous que vous êtes connecté avec ce profil.