Désigner un pilote

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

La désignation d'un délégué à la protection des données est obligatoire en 2018 si :

- Vous êtes un organisme public ;
- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, il est fortement recommandé de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen. Le délégué constitue un atout majeur pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des données et réduire les risques de contentieux.

Le rôle du délégué à la protection des données

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- **d’informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- **de contrôler le respect du règlement** et du droit national en matière de protection des données ;
- **de conseiller l’organisme** sur la réalisation d’études d'impact sur la protection des données et d’en vérifier l’exécution ;
- **de coopérer avec l’autorité de contrôle** et d’être le point de contact de celle-ci.

Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :

- **s’informer** sur le contenu des nouvelles obligations ;
- **sensibiliser** les décideurs sur l’impact de ces nouvelles règles ;
- **réaliser l’inventaire** des traitements de données de votre organisme ;
- **concevoir** des actions de sensibilisation ;
- **piloter** la conformité en continu.

Cartographier vos traitements de données personnelles

Pour mesurer concrètement l’impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en oeuvre. La tenue d'un registre des traitements vous permet de faire le point.

Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s’assurer que ces traitements respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du règlement sur votre activité et de répondre à cette exigence, vous devez au préalable recenser précisément :

- Les différents traitements de données personnelles,
- Les catégories de données personnelles traitées ;
- Les objectifs poursuivis par les opérations de traitements de données ;
- Les acteurs (internes ou externes) qui traitent ces données. Vous devrez notamment clairement identifier les prestataires sous-traitants afin d'actualiser les clauses de confidentialité ;
- Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Pour chaque traitement de données personnelles, posez-vous les questions suivantes :

QUI ?

- Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ;
- Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme ;
- Etablissez la liste des sous-traitants.

QUOI ?

- Identifiez les catégories de données traitées
- Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions)

POURQUOI ?

- Indiquez la ou les finalitéspour lesquelles vous collectez ou traitez ces données (exemple : gestion de la relation commerciale, gestion RH…).

OÙ ?

- Déterminez le lieu où les données sont hébergées.
- Indiquez quels pays les données sont éventuellement transférées.

JUSQU'À QUAND ?

- Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

COMMENT ?

- Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

Prioriser les actions à mener

Sur la base du registre des traitements, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de votre organisme, vous devez, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir.

Cette priorisation peut être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et vous permettront de progresser rapidement.

Points d'attention quels que soient vos traitements

1. Assurez-vous que **seules les données strictement nécessaires** à la poursuite de vos objectifs sont collectées et traitées.
2. Identifiez **la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
3. Révisez vos **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)
4. Vérifiez que vos **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
5. Prévoyez les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
6. Vérifiez les **mesures de sécurité** mises en place.

Points d'attention nécessitant une vigilance particulière

VOUS TRAITEZ CERTAINS TYPES DE DONNÉES

- des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- des données concernant la santé ou l'orientation sexuelle,
- des données génétiques ou biométriques,
- des données d'infraction ou de condamnation pénale,
- des données concernant des mineurs.

VOTRE TRAITEMENT A POUR OBJET OU POUR EFFET

- la surveillance systématique à grande échelle d'une zone accessible au public ;
- l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

VOUS TRANSFÉREZ DES DONNÉES HORS DE L'UNION EUROPÉENNE

- vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne ;
- dans le cas contraire, encadrez vos transferts.

> En savoir plus

Si vos traitement répondent à ces caractéristiques, des mesures particulières peuvent s'appliquer (exemple : étude d'impact sur la protection des données (PIA), information renforcée, recueil du consentement, autorisation préalable, clauses contractuelles,). Une analyse approfondie de la loi informatique libertés et du règlement

Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (en anglais, Data protection impact assessment ou Privacy Impact Assessment).

Qu’est-ce qu’une analyse d'impact sur la protection des données (PIA) ?

C’est une étude aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD. Un PIA est un outil d’évaluation d’impact sur la vie privée. Il repose sur 2 piliers :

1. les principes et droits fondamentaux, « non négociables », fixés par la loi. Ils ne peuvent faire l’objet d’aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;
2. la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d’organisation appropriée pour protéger les données personnelles.

Un PIA contient :

- Une description du traitement étudié et de ses finalités.
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- une évaluation des risques pour les droits et libertés des personnes concernées les mesures envisagées pour faire face aux risques.

Quand mener une analyse d'impact sur la protection des données (PIA) ?

De manière générale, réaliser un PIA est une bonne pratique pour s’assurer de créer un traitement conforme au RGPD et respectueux de la vie privée, que celui-ci soit susceptible ou non d’engendrer des risques élevés sur la vie privée.

Le PIA doit être réalisé avant la mise en œuvre du traitement. C’est un processus itératif, les analyses doivent être revues et corrigées de manière régulière, en particulier lors de changements majeurs des modalités d’exécution du traitement.

Mener un PIA est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (Article 35 du RGPD). Pour vous aider à déterminer si votre traitement est

susceptible d'engendrer des risques élevés, les 9 critères suivant sont définis dans les lignes directrices du G29 :

1. Evaluation ou notation;
2. Décision automatisée avec effet juridique ou effet similaire significatif;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement personnel ;
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si votre traitement rencontre au moins 2 de ces critères, alors il est vivement conseillé de faire un PIA.

Qui participe à l'élaboration de l'analyse d'impact ?

- **Le responsable de traitement** : valide Le PIA et s'engage à mettre en œuvre le plan d'action défini dans le PIA ;
- **Le délégué à la protection des données :** élabore le plan d'action et se charge de vérifier son exécution ;
- **Le(s) sous-traitant(s) :** fournit les informations nécessaires à l'élaboration du PIA ;
- **Les métiers** (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre) : aident à la réalisation du PIA en fournissant les éléments adéquats ;
- **Les personnes concernées** : donnent leurs avis sur le traitement.

est nécessaire pour déterminer les mesures à mettre en œuvre.

Organiser les processus internes

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

Organiser les processus implique notamment :

- **de prendre en compte de la protection des données personnelles dès la conception** d'une application ou d'un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données). Pour cela, appuyez-vous sur les conseils du délégué à la protection des données;
- **de sensibiliser et d'organiser la remontée d'information** en construisant notamment un plan de formation et de communication auprès de vos collaborateurs ;
- **de traiter les réclamations et les demandes des personnes concernées quand à l'exercice de leurs droits** (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen) ;
- **d'anticiper les violations de données** en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

Documenter la conformité

10 mars 2017

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Votre dossier devra notamment comporter les éléments suivants :

LA DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants)
- **Les analyses d'impact sur la protection des données** (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes
- **L'encadrement des transferts** de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications)

L'INFORMATION DES PERSONNES

- **Les mentions d'information**
- Les modèles de **recueil du consentement des personnes concernées**,
- Les procédures mises en place pour **l'exercice des droits**

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- **Les contrats avec les sous-traitants**
- Les procédures internes **en cas de violations de données**
- Les preuves que les personnes concernées **ont donné leur consentement** lorsque le traitement de leurs données repose sur cette base.

VOUS AUREZ FRANCHI CETTE ÉTAPE SI

- Votre documentation démontre que vous respectez les obligations prévues par le règlement européen