Règlement européen

sur la protection des données personnelles

se préparer en 6 étapes

En mai 2018, le règlement européen sera applicable.
De nombreuses formalités auprès de la CNIL vont disparaître.
En contrepartie, la responsabilité des organismes sera renforcée.
Ils devront en effet assurer une protection optimale des données
à chaque instant et être en mesure de la démontrer
en documentant leur conformité.

Désigner
un pilote

Cartographier
vos traitements de
données personnelles

Prioriser
les actions

Gérer
les risques

Organiser
les processus internes

Documenter
la conformité

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

ÉTAPE 1

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 (CIL), 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 :

- d'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.

Sur cnil.fr
Pour préparer la désignation de votre futur délégué, désignez un CIL.

Vous aurez franchi cette étape si :

- ☐ vous avez désigné au sein de votre structure un pilote (un CIL qui a vocation à être désigné délégué), chargé de mettre en œuvre la conformité au règlement sur la base d'une lettre de mission,
- ☐ vous lui avez affecté les moyens humains et financiers pour mettre en œuvre ses missions.

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 œuvre. 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 finalités pour lesquelles vous collectez ou traitez ces données (par exemple : gestion de la relation commerciale, gestion RH...).

OÙ ?
- Déterminez le lieu où les données sont hébergée.
- Indiquez quels pays les données sont éventuellement transférées.

JUSQU'À QUAND ?
Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

COMMENT ?
Préciser les 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.

Sur cnil.fr
Pour vous familiariser avec le futur registre des traitements de donnée personnelles, téléchargez notre modèle de registre.

Vous aurez franchi cette étape si :

- ☐ vous avez rencontré les services et les entités qui traitent des données personnelles,
- ☐ vous avez établi la liste des traitements par finalité principale (et non par outil ou applicatif utilisé) et les types de données traitées,
- ☐ vous avez identifié les sous-traitants qui interviennent sur chaque traitement,
- ☐ vous savez à qui et où les données sont transmises,
- ☐ vous savez où sont stockées vos données,
- ☐ vous savez combien de temps ces données sont conservées.

ÉTAPE 3

Prioriser les actions

Sur la base du registre des traitements de données personnelles, 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 les traitements de données

- **Assurez-vous** que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
- **Identifiez** la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
- **Révisez** vos mentions d'information afin qu'elles soient conformes aux exigences du règlement
- **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.
- **Prévoyez** les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement…).
- **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 de données personnelles a 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.

Sur cnil.fr

Pour préparer les modèles de contrats avec vos sous-traitants, consultez nos modèles de clauses.

Vous aurez franchi cette étape si :

- ☐ vous avez mis en place les premières mesures pour protéger les personnes concernées par vos traitements,
- ☐ vous avez identifié les traitements à risque.

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 étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA).

L'étude d'impact relative à la protection des données permet :

- **de bâtir** un traitement de données personnelles ou un produit respectueux de la vie privée,
- **d'apprécier** les impacts sur la vie privée des personnes concernées,
- **de démontrer** que les principes fondamentaux du règlement sont respectés.

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

- avant de collecter des données et de mettre en œuvre le traitement,
- sur tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques.

Que contient une étude d'impact sur la protection des données (PIA) ?

- **une description** du traitement et de ses finalités,
- **une évaluation** de la nécessité et de la proportionnalité du traitement,
- **une appréciation** des risques sur les droits et libertés des personnes concernées, les mesures envisagées pour traiter ces risques et se conformer au règlement.

Les outils pour vous aider

La CNIL met à votre disposition sur son site les guides PIA, un catalogue de bonnes pratiques qui vous aide à déterminer les mesures proportionnées aux risques identifiés, en agissant sur :

- **les « éléments à protéger »** :
  minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits, ect.
- **les « impacts potentiels »** :
  sauvegarder les données, tracer l'activité, gérer les violations de données ect.
- **les « sources de risques »** :
  contrôler les accès, gérer les tiers, lutter contre les codes malveillants ect.
- **les « supports »** :
  réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier ect.

Pour traiter un risque identifié et le réduire à un niveau acceptable, l'utilisateur des guides peut sélectionner une ou plusieurs mesures appropriées. Il est impératif d'adapter les mesures au risque et au contexte particulier du traitement considéré. Des études de cas sur la géolocalisation de véhicules d'entreprise et la gestion des patients d'un cabinet de médecine du travail, réalisées par le Club EBIOS, illustrent la mise en application de ces outils.

Sur cnil.fr
Pour expérimenter la méthodologie du PIA, téléchargez les guides PIA de la CNIL.

Vous aurez franchi cette étape si :

- ☐ vous avez mis en place des mesures permettant de répondre aux principaux risques et menaces qui pèsent sur la vie privée des personnes concernées par vos traitements.

ÉTAPE 5

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 de données personnelles (par exemple : 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** 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,
- **sensibiliser et d'organiser** la remontée d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs,
- **traiter** les réclamations et les demandes des personnes concernées quant 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),
- **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.

Sur cnil.fr

Dans l'attente du téléservice de notification de violations de données personnelles (disponible en mai 2018 sur cnil.fr), consultez d'ores et déjà le formulaire de notification de violations de données personnelles, réservé à ce jour aux fournisseurs de services de communications électroniques au public.

Vous aurez franchi cette étape si :

- ☐ les réflexes de la protection des données sont acquis et appliqués au sein des services qui mettent en œuvre des traitements de données,
- ☐ votre organisme sait quoi faire et à qui s'adresser en cas d'incident.

Documenter la conformité

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.

Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement. Les mesures organisationnelles et techniques sont réexaminées et actualisées si nécessaire.

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 ; voir étape 4) 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.

Les ressources

Désigner un pilote

> Le CIL et le futur délégué à la protection des données [PAGE WEB]
> Guide pratique de la prise de fonction du CIL [PDF]
> Devenir délégué à la protection des données [PAGE WEB]

Cartographier vos traitements

> Modèle de registre règlement européen [EXCEL]
> Exemple de fiche de registre CIL [PDF]
> Demandez la liste des fichiers déclarés à la CNIL [FORMULAIRE]

Prioriser les actions

> Guide sécurité des données personnelles [PDF]
> Modèle de Clause de contrat sous-traitant [PDF]
> Clause contrat sous-traitant pour maintenance ou télémaintenance [PDF]

Gérer les risques

> PIA-2, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée [PDF]
> PIA-3, les bonnes pratiques : Mesures pour traiter les risques sur les libertés et la vie privée [PDF]

Organiser les processus internes

> Le référentiel du label Gouvernance [DOCX]
> La notification de violations [PAGE WEB]

Retrouvez toutes les ressources dans la rubrique « Règlement européen » du site de la CNIL