Fideliance Digital

RGPD : quelles sont les actions à mettre en place?

Nous sommes tous concernés aussi bien dans votre vie professionnelle que personnelle

Le **R**ègleme**n**t **G**énéral sur la **P**rotection des **D**onnées n° 679/2016 (***G**eneral **D**ata **P**rotection **R**egulation)*, remplacera la **directive** 95/46/CE (publiée en 1995). Cette directive a servi, en France, de fondement à la loi Informatique & Libertés.

CNIL.

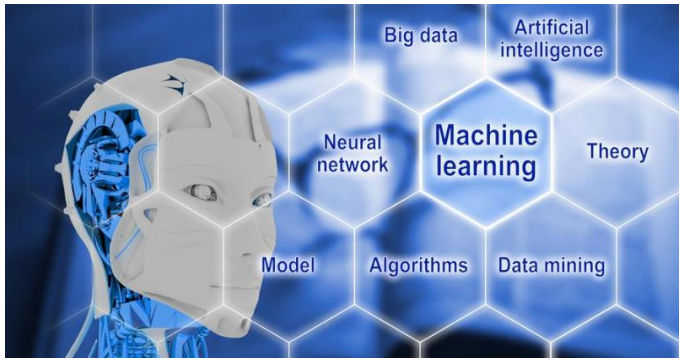
Mise en œuvre du

RGPD

Big Data, Objets connectés, IA …

Fideliance Digital

L'analyse des données est en train de révolutionner notre société.
Toutes les **données que nous produisons chaque jour sont répertoriées et réutilisées**, que ce soit les données émises par nos **téléphones, montres connectées, ordinateurs, voitures** …

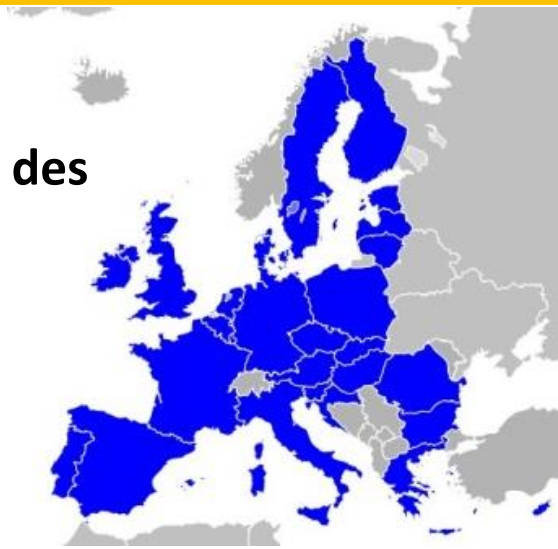


90% des données existantes aujourd'hui ont été créées au cours des 3 dernières années.

80% des données à caractères personnel sont possédées par les GAFA

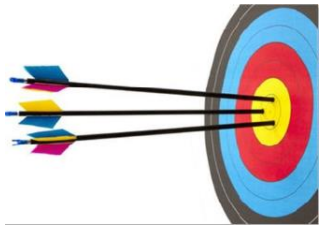
Ex : acquisition illégale des données de 50 millions d'utilisateurs de **Facebook** par Cambridge Analytica pour influencer la présidentielle aux Etats-Unis !

Quelles sont les entreprises concernées ?



Les règles du RGPD s'appliqueront **à toutes les entreprises privées ou publiques des 28 Etats membres** de l'Union européenne.

Plus précisément, aux entreprises :



- Proposant des **biens et services** sur le marché de l'UE.
- **Collectant ou traitant des données à caractère personnel sur les résidents de l'UE**.

A noter que le règlement s'appliquera également aux **entreprises non implantées en UE**, dès lors qu'elles collectent et traitent des données personnelles sur des résidents de l'UE.

Mais qu'est-ce qu'une donnée personnelle ?

Il s'agit de toute information relative à une **personne physique identifiée ou susceptible de l'être**, directement ou indirectement, par référence à un numéro d'identification (ex : N° de sécurité sociale) ou à un ou plusieurs éléments qui lui sont propres :

- Nom, prénom, adresse, casier judiciaire
- Sexe, âge, situation familiale
- Diplôme, poste, salaire
- Goûts, habitudes de consommation …
- Etat de santé, maladies
- Codes de carte bancaire, numéros de comptes, RIB …
- SMS, photos, contacts …
- Mails, carnets d'adresse, adresse IP, Réseaux sociaux …
- Géolocalisation

Interne : RH …

Externe : clients, Frs …

Cas d'une donnée **non personnelle**

Ex l'anonymisation

Résultats de notre enquête de satisfaction !

92% de nos clients sont « satisfaits » de nos prestations dont 68% « très satisfaits »

97% sont « satisfaits » de leur relation avec leur collaborateur dont 82% « très satisfaits »

89% sont prêts à recommander Fideliance

Votre reconnaissance est notre meilleure récompense

C’est quoi cette nouvelle règlementation ?

Les changements clés

Renforcement des droits des personnes et des obligations des établissements.

Cela passe par **6 principes clefs** :

Licéité du traitement

- ✓ **Consentement** au traitement par la personne concernée
- ✓ Nécessité pour l'exécution **d'un contrat** ou de mesures précontractuelles
- ✓ Nécessité pour le **respect d'une obligation légale**
- ✓ Nécessité pour la **sauvegarde d'intérêts vitaux**
- ✓ Exécution d'une **mission d'intérêt public**
- ✓ Nécessité **aux fins des intérêts légitimes** du Responsable du Traitement ou d'un tiers

- Règlementation renforcée

Transparence explicite des données collectées pour des finalités précises et ne peuvent pas être traitées ultérieurement pour d'autres finalités

- Règlementation renforcée

Les changements clés

Protection des données

garantir que la protection de la vie privée soit intégrée dans les nouvelles applications à leur création (PIA, privacy by design, anonymisation, pseudonymisation …)

- Règlementation renforcée

Sous-traitants

Obligation de garantir le respect des dispositions par l'ensemble de ses sous-traitants

- Règlementation nouvelle

Les changements clés

Portabilité

Possibilité de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers (Ex : changement de fournisseur)

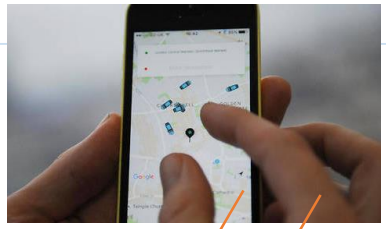
- Règlementation nouvelle

Modification et effacement

Possibilité de demander l'effacement de ses données personnelles (droit à l'oubli)

- Règlementation maintenue

Notifier la CNIL, sous 72h *en cas de risque réel d'atteinte à la protection de la vie privée.*



Uber, Yahoo …

Opportunités

Pourquoi c'est une opportunité pour vous?

Si la **DATA** est le nouveau pétrole

Alors la **CONFIANCE** est la nouvelle monnaie

Le RGPD permet de définir un cadre pour instaurer cette **confiance et gérer votre PATRIMOINE DIGITAL**

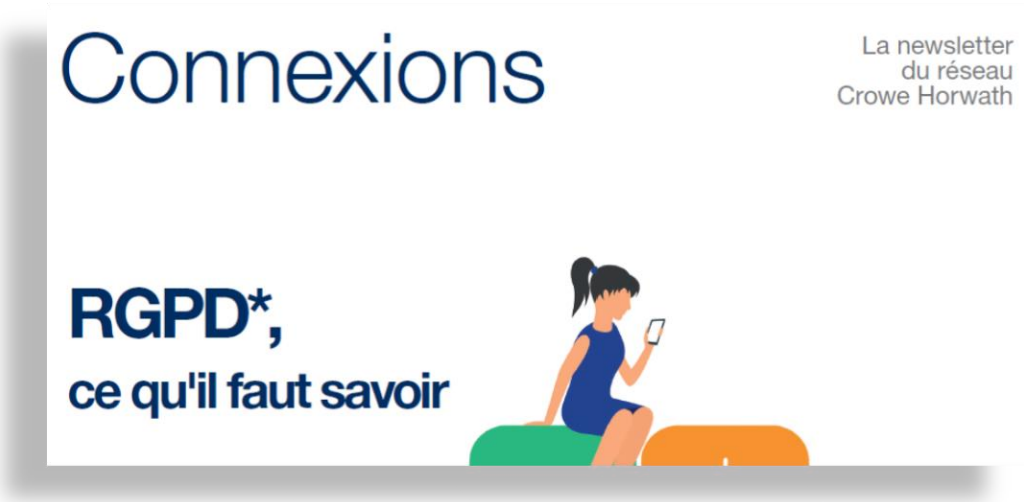
Pourquoi c'est une opportunité pour vous ?

S'engager dans une démarche globale vertueuse en ce qui concerne la vie privée dans la collecte et le traitement des données

- Valoriser votre entreprise
- Eviter les risques sur l'image de l'entreprise, sa réputation (exemple : Uber, Yahoo …)
- Etre éligible pour répondre à certains appels d'offre exigeant d'être conforme
- Optimiser la protection de votre entreprise face aux attaques
- Rationaliser les processus de gestion des données
- Opportunité de business en instaurant un renouveau dans la relation client
- Et bien sur éviter une pénalité (jusqu'à 20 millions € ou 4% du CA annuel mondial)

Des questions ?

La newsletter
« Connexions » dédié
RGPD



Plaquette
FIDELIANCE DIGITAL

Les actions attendues pour être conforme

… à faire en continu

Il faut appliquer les informations du registre :

- **Le Respect des droits des personnes concernées** (droit d'accès, droit d'opposition, de rectification, de limitation, d'effacement, de portabilité…)
- **Le devoir de transparence:** Faire preuve de transparence en veillant à toujours fournir une information claire et intelligible et obtenir l'obtention du consentement (en garder la preuve)

Fideliance Digital

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 à des 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.**

Désigner un pilote

- **L'obligation de désignation d'un Data Protection Officer** (« Délégué à la Protection des Données »). Doté d'un rôle très important, le DPO sera chargé de piloter la gouvernance des données, de contrôler la conformité de l'entreprise avec le GDPR et de conseiller le responsable des traitements

Obligatoire pour les entreprises réalisant des traitements de données sensibles, à grande échelle, ou systématique.

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 nécessaires pour mettre en œuvre ses missions.

Sensibiliser

- Mise en place d'une Charte Informatique (ajuster par rapport à vos spécificités) : https://www.cnil.fr/sites/default/files/typo/document/20100730-MOD-CHARTE_INFORMATIQUE_CIL-VD.pdf
- Engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel : https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs
- Informer clairement tous les employés et obtenir leur consentement exprès. Ce qui implique sans doute de revoir les clauses de vos contrats de travail pour répondre aux exigences du RGPD (ou rédiger une note d'information à faire signer si possible par chaque travailleur)
- Revoir les contrats fournisseurs
- Les impacts concernant la prospection commerciale par mailing : https://www.cnil.fr/fr/la-prospection-commerciale-par-courrier-electronique
- Mettre à jour vos documents stratégiques avec vos clients, comme les mentions légales ou les CGV exemple : https://www.donneespersonnelles.fr/conditions-generales-de-vente

Fideliance Digital

3 ATELIERS

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

Cartographier
vos traitements de données personnelles

Fideliance Digital

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 traitement de données,
- **les acteurs** (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires sous-traitants,
- **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 hébergées.
- Indiquez vers quels pays les données sont éventuellement transférées.

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

COMMENT ?
Précisez les mesures de sécurité 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 données personnelles, téléchargez notre modèle de registre.

Indiquer le type de support : papier, informatique, audio, vidéo …

Cartographier
vos traitements de données personnelles

Fideliance Digital

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

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.

Prioriser les actions

Fideliance Digital

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 traitement de données,
- **les acteurs** (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires sous-traitants,
- **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 hébergées.
- Indiquez vers quels pays les données sont éventuellement transférées.

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

COMMENT ?
Précisez les mesures de sécurité 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 données personnelles, téléchargez notre modèle de registre.

Crypter vos fichiers ou mettre des mots de passe complexe

Stocker vos données sur des DataCenter en France

Sécuriser votre parc informatique (anti-virus, firewall ...)

Prioriser les actions

Fideliance Digital

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 relatives à 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 vos contrats avec vos sous-traitants, consultez notre modèle de clause de confidentialité,

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.

Fideliance Digital

L'étude d'impact sur 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.

PIA = **P**rivacy **I**mpact **A**ssessment

Les outils pour vous aider

La CNIL met à votre disposition sur son site les guides PIA, catalogues 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, etc.
- **les « impacts potentiels » :**
  sauvegarder les données, tracer l'activité, gérer les violations de données etc.
- **les « sources de risques » :**
  contrôler les accès, gérer les tiers, lutter contre les codes malveillants etc.
- **les « supports » :**
  réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier etc.

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.

Annexes

8 droits pour les individus

Article 7

Consentement explicite

Articles 11 à 14

Information de la personne

Article 15

Droit d'accès

Article 16

Droit de rectification

Article 17

Droit à l'oubli

Articles 20

Droit à la portabilité

Article 21

Droit d'opposition

Article 22

Décisions automatisées (profilage)

8 obligations pour les organisations

Article 5

Responsabilité et « Accountability »

Articles 25

Privacy by Design by Default

Article 30

Registre des traitements

Article 32

Sécurisation des traitements

Articles 33 & 34

Fuites de données

Articles 35

Data Privacy Impact Assessment (DPIA)

Articles 37 à 39

Data Protection Officer (DPO)

Articles 44 à 49

Transferts de données

Vos contacts

Christian GABENESCH
christian.gabenesch@fideliance.fr

Xavier LARBALETTE
xavier.larbalette@fideliance.fr

Votre contact : 01.64.98.74.25

N’hésitez pas à nous contacter pour échanger sur vos besoins !