Ligue de l'Enseignement des Côtes d'Armor

La mise en conformité au RGPD
Ensemble pour avancer

J. LE NOUVEL – Délégué à la Protection des Données – Amicale Laïque de Ploeuc-sur-Lié
Le 5 novembre 2020

FÉDÉRATION CÔTES D'ARMOR
la ligue de l'enseignement
un avenir par l'éducation populaire

Fédération d'éducation populaire
mouvement complémentaire de l'école publique

Source : *Site Internet de la* CNIL.

RGPD

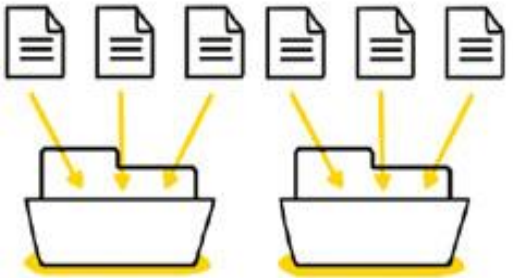
PASSER À L'ACTION

en 4 étapes

1

Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

3

Respectez les droits des personnes

4

Sécurisez vos données

CNIL.

Sommaire

- Qu'est-ce que le RGPD ?
- Qu'est-ce qu'une donnée personnelle ?
- A qui s'adresse-t-il ?
- Quelles sont les obligations des responsables des traitements ?
- Quelles sont les droits des personnes concernées ?
- Comment désigner un Délégué à la Protection des Données (DPD) ?
- Engager la démarche
- Les droits d'accès des personnes et les sanctions accrues

De quand date la protection des données personnelles ?

Le Monde – 21 mars 1974

• • • LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

« Safari » ou la chasse aux Français

☞ *Création de la loi informatique et liberté 6 janvier 1978*

FÉDÉRATION CÔTES D'ARMOR
la ligue de l'enseignement
un avenir par l'éducation populaire

Fédération d'éducation populaire
mouvement complémentaire de l'école publique

Le RGPD, c'est quoi ?

- C'est un règlement Européen qui **s'applique dès le 25 mai 2018**
- Il **ne nécessite pas d'adaptation des lois nationales** pour les Etats membres
- Il régit un ensemble de règles permettant aux personnes concernées d'exercer auprès des responsables des traitements un certain nombre de recours concernant la protection de leurs données personnelles
- Il régit les obligations du responsable des traitements, co-responsables et de ses sous-traitants

A qui le RGPD s'adresse-t-il ?

Sont **soumises au RGPD tous les types d'associations,** qu'il s'agisse d'une association loi de 1901, d'une association de gestion agréée , d'une association reconnue d'utilité publique ou d'une association non déclarée ou association de fait qui :

- possèdent et traitent un fichier comportant des informations personnelles sur ses membres ;
- possèdent une base de données contenant le contact de ses membres pour l'envoi de mail ou de newsletter ;
- conservent les données personnelles de ses bénévoles ou employés.

Il s'adresse également à fortiori à toutes les **entreprises** et **collectivités**.

Il ne s'adresse pas aux particuliers (carnet d'adresses, photographies, etc.)

Il ne concerne que **les personnes physiques** et **non les personnes morales.**

Qu'est-ce qu'une donnée personnelle ?

« Une donnée personnelle permet d'identifier directement ou indirectement une personne physique »

Exemples de données : nom, prénom, photographie, numéro de sécurité sociale, date et lieu de naissance, adresse IP, numéro de téléphone, etc.

Autre exemple : Mme X est la seule médecin de la commune de Y. Elle a un seul fils. Donc, en disant « Le fils du médecin de la commune de Y … », cela constitue une donnée à caractère personnel permettant d'identifier indirectement une seule et unique personne.

Cas particulier : Les données sensibles

- Par défaut, **la collecte des données sensibles** est **INTERDITE**. Il s'agit de :
  - Les origines raciales ou ethniques
  - Les opinions politiques, philosophiques ou religieuses
  - L'appartenance syndicale
  - La santé
  - La vie sexuelle
  - Les données génétiques et biométriques
- Le consentement express (libre, spécifique, éclairé et univoque) spécifique de chaque utilisateur est obligatoire pour pouvoir les collecter (1er du I de l'article 8 de la loi informatique & libertés du 6 janvier 1978) et Article 4 N° 11 du RGPD.

Quelles sont les données concernées ?

- Il concerne les **données personnelles** qu'elles soient **informatisées ou non** !
- Il concerne les structures dont :
  - Les activités se passent sur le territoire de l'Union Européenne : **la territorialité**
  - Les clients, prospects ou adhérents (personnes concernées) sont situés sur le territoire de l'Union Européenne : **le ciblage**

Les principes à respecter

- **Article 5 du RGPD : Principes relatifs au traitement des données à caractère personnel**

1. Les données à caractère personnel doivent être :

a) traitées de manière **licite, loyale et transparente au regard de la personne concernée** (licéité, loyauté, transparence) ;

b) collectées pour des **finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

c) **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) **exactes et, si nécessaire, tenues à jour**; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude)

Les principes à respecter

- **Article 5 du RGPD : Principes relatifs au traitement des données à caractère personnel**

1. Les données à caractère personnel doivent être :

e) **conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées**; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à **garantir une sécurité appropriée des données à caractère personnel**, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Les principes à respecter

- **Article 6 du RGPD : Licéité du traitement**

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

a) la personne concernée a **consenti au traitement de ses données à caractère personnel** pour une ou plusieurs **finalités** spécifiques ;

b) le traitement est nécessaire à l'exécution d'un **contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) le traitement est nécessaire au respect d'une **obligation légale** à laquelle le responsable du traitement est soumis ;

Les principes à respecter

. Article 6 du RGPD : Licéité du traitement

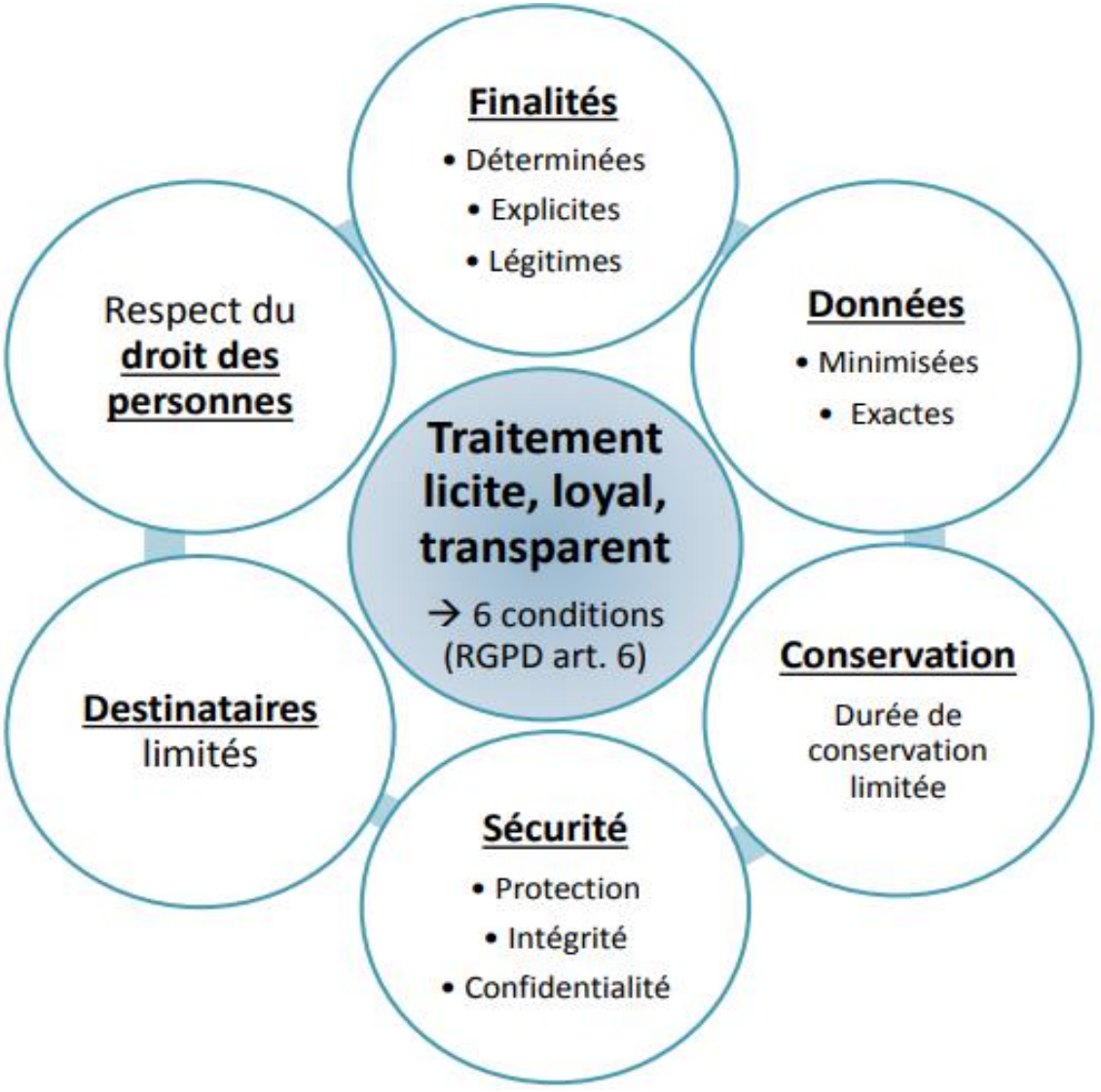
1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

d) le traitement est **nécessaire à la sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique ;

e) le traitement est **nécessaire à l'exécution d'une mission d'intérêt public** ou relevant de **l'exercice de l'autorité publique** dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des **intérêts légitimes poursuivis par le responsable du traitement** ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Les principes à respecter



FÉDÉRATION CÔTES D'ARMOR
la ligue de l'enseignement
un avenir par l'éducation populaire

Source : Centre de Gestion de la Fonction Publique Territoriale des Côtes d'Armor

Le responsable du traitement

– **Art. 4 Alinéa 7 : Le responsable de traitement**

*« **responsable du traitement**», **la personne physique ou morale**, l'autorité publique, le service ou un autre organisme **qui**, seul ou conjointement avec d'autres, **détermine les finalités et les moyens du traitement**; … »*

La Cnil le précise :

« Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la **personne morale incarnée par son représentant légal**. »

☞ **En somme, pour l'association, il s'agit de la personne morale présidente de l'association.**

Le responsable du traitement

. Article 24 du RGPD : Responsabilité du responsable du traitement

1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.**

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la **mise en œuvre de politiques appropriées en matière de protection des données** par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Les finalités du traitement

. Les finalités du traitement doivent être ***déterminées*** :

– Pourquoi collecter telle données ? Il faut se poser la question de « A quoi cela va me servir ? »

– En se posant cette question, vous vous affranchissez de recueillir, saisir et tenir à jour des données inutiles ! Vous gagnez ainsi du temps.

– Ces données doivent être adéquat et à jour !

Les finalités du traitement

- Les finalités du traitement doivent être ***explicites*** :
  - Vous devez, lors de la collecte des données, informer du traitement qu'il va être fait de celles-ci.
- Mentions dans les formulaires à adapter à chaque situation
- Laisser le choix aux personnes de vous donner telle ou telle données (obligatoires* ou facultatives) en fonction des traitements que vous devez réaliser
- Exposer la possibilité d'avoir accès aux informations les concernant et à qui s'adresser pour ce faire (cf. Droit des Personnes)
- **Cas des mineurs :** les mineurs de + de 15 ans peuvent dans certains cas éviter l'autorisation parentale (à voir au cas par cas).

Les finalités du traitement

- Les finalités du traitement doivent être ***légitimes*** :

  – Certaines activités sont régies par un cadre légal auxquels vous devez vous conformer.

  – Les textes imposent le recueil de certaines données obligatoires pour pouvoir accéder à certains services. Sans ces données, vous ne pouvez traiter les demandes,

- Exposer ces textes légaux pour assurer une transparence dans votre démarche obligatoire

Les données recueillies

- La collecte des données doit être ***minimaliste et adéquate*** (« A quoi vont me servir ces données ? »)
- Le recueil de données impose la gestion de ***l'exactitude*** de celles-ci (mise à jour)

☞ ***Vous ne devez pas recueillir des données inutiles : VOUS DEVEZ LES METTRE A JOUR !***

La conservation des données

. **Trois aspects sont à prendre en compte :**

– La durée de conservation légale (factures, fiches de paie, etc.) ;

– La durée de conservation des données que vous souhaitez mettre en œuvre de façon particulière ;

– L'anonymisation des données (ex : à des fins statistiques)

. Dans les 3 cas, il est conseiller d'en **informer les personnes au moment du recueil des informations**.

. **Exemples de délais de conservation des données :** https://www.economie.gouv.fr/particuliers/delais-conservation-papiers-personnels

La protection des données

Communiquer et sensibiliser au sein de votre association

L'intégrité des données :

En l'occurrence, il faut s'assurer que les données ne puissent pas être corrompues par qui que ce soit ou quelque syste
que ce soit.

La confidentialité des données :

Concernant certaines données, elles n'ont pas vocation à être connues de certaines personnes, notamment les données sensibles (données de paie, de santé, plan d'accueil individualisé, etc.).

La sécurité :

- Assurer la gestion des droits d'accès et gérer la traçabilité des accès ;
- Mettre en place un système de sauvegarde sécurisé ;
- Identifier chaque utilisateur par des identifiant et mot de passe personnels ;
- Gérer les mouvements des utilisateurs (départ, arrivée, changement d'affectation au sein de la structure).

Gérer les droits et habilitations applicatives des personnes

La protection des accès

- **Gérez vos mots de passe :**
  - Utilisez de mots de passe complexe (MAJUSCULES, minuscules, chiffres et caractères spéciaux #@/§ etc.)
  - Utilisez des moyens simples de les retrouver : « J'ai acheté un pain pour Marie » ➔ Ght1P1pourM@rie
  - Changez les régulièrement
  - Utilisez des logiciels adaptés : exemple KeyPass
  - Ne les conservez pas sur un post-it, dans un fichier ou sur un cahier …
  - Ne communiquez jamais un mot de passe par courriel
  - N'enregistrez jamais vos mots de passe comme proposé par vos navigateurs préférés
  - **France Connect** pour les sites institutionnels ou intégrant les interfaces France Connect : https://franceconnect.gouv.fr/
- **Sécurisez vos accès à vos applications et vos accès :**
  - Utilisez le protocole HTPPS (ou TLS) pour crypter de votre poste de travail au serveur les données transmises
  - Utilisez un VPN pour cacher l'adresse IP de votre réseau professionnel, associatif ou personnel

Les destinataires des données

- Certaines données ne vous concernent pas uniquement. Vous êtes à même de les communiquer à des tiers.
- Vous devez en informer les personnes explicitement.
- *Exemple :*
  - Gestion de la paie ;

    Envoi de la fiche de paie

    Virement : destinataire : banque

    Cotisations : URSSAF, etc.

Les destinataires des données

- **Le cas particulier des sous-traitants** (art. 28 du RGPD)
  - « Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée. »
  - Il doit tout mettre en œuvre pour assurer la sécurité et la confidentialité des données avec l'aval du responsable des traitements (clauses des contrats)
  - Renforcement de la responsabilité des sous-traitants

Les destinataires des données

- Cas particulier des ***sites internet*** :

– Certains sites internet recueillent des données par le biais de COOKIES ou de TRACEURS.

– Certaines données recueillies peuvent l'être à l'insu de la personne connectée. Ces pratiques sont à proscrire. Il convient d'en informer l'utilisateur avec un bandeau lui précisant le recueil de ces informations et lui offrir la possibilité de s'y opposer de manière simple et intelligible.

–Tout recueil d'information en dehors de l'union européenne est interdit sauf consentement éclairé et expresse des personnes concernées. Vous devez absolument en informer l'utilisateur et recueillir sont consentement (ex : Recaptcha et Google Analytics).

– Il est préconisé de disposer d'un hébergement au sein d'un état de l'union européenne (y compris les sauvegardes)

Le respect du droit des personnes

- **Les différents droits sont (plus d'informations) :**
  - Le droit d'information
  - Le droit d'accès
  - Le droit de rectification
  - Le droit d'opposition
  - Le droit d'effacement
  - Le droit de portabilité
  - Le droit de limitation

Les dispositions d'application du droit des personnes

- Le délai de réponse à une demande est de 1 mois à compter de la réception de celle-ci.
- Une procédure doit être établie pour le traitement de la demande et les modalités de réponse (Exemple : données médicales ⇒ présence du Médecin).
- Il faudra s'assurer de l'identité du demandeur ou de l'ayant droit.
- Assurer la traçabilité des demandes (DPD ou référent de l'association)

Les plaintes des personnes concernées

- Les plaintes auprès de la CNIL se font en ligne, suivez le guide. Le plaignant devra fournir l'ensemble des échanges avec le responsable des traitements avec les délais réels des échanges.
- Conservez toutes les **traces de tous les échanges**, elles seront utiles en cas de plainte et de contrôle.

☞ Pour porter plainte, c'est par ici.

https://www.cnil.fr/fr/plaintes/

Procédure en cas de violation de données personnelles

« Le RGPD impose de notifier à la CNIL les violations présentant un risque pour les droits et libertés des personnes et, dans certains cas, lorsque le risque est élevé, aux personnes concernées. » *Source Site internet de la CNIL*

On entend par « violation », un perte :

- de **disponibilité**
- **d'intégrité**
- de **confidentialité** de données personnelles

que cette perte soit **accidentelle** ou **illicite.**

Pour notifier aux responsables de traitement pour notifier à la CNIL : cliquez-ici

Délais de notification :

- **Une notification initiale dans un délai de 72 heures** si possible à la suite de la constatation de la violation ;
- Si le **délai de 72 heures est dépassé,** vous devrez expliquer, lors de votre notification, les motifs du retard **;**
- Enfin, **une notification complémentaire** dès lors que les informations complémentaires sont disponibles.

En somme ...

« On dit ce qu'on fait et on fait ce qu'on dit »

La mise en œuvre de la conformité

La démarche progressive et itérative, associez les personnes de terrain, au plus près de opérations réalisées

- **Désignez une personne référente** missionnée pour assurer la coordination des opérations ;
- **Sensibilisez l'ensemble des membres de l'association** gérant des données personnelles ;
- **Répertoriez tous les traitements de données à caractère personnel** dans un fichier dédié ;
- **Pour chaque traitement**, identifiez les processus de gestion, les différents acteurs (Personnes de l'association, destinataires des données, etc.), identifiez chaque donnée concernée pour une personne physique y compris les données sensibles ;
- **Complétez** ensuite **les fiches registres associées à chaque traitement**, elles constitueront votre registre ; Elles seront versionnées de façon à les faire évoluer en cas de besoin (exemple ici)
- **Documentez** votre démarche de mise en conformité (ex : cette réunion est une sensibilisation que vous avez suivi et donc, pour certain, vous avez lancé une démarche vers la mise en conformité)

La mise en œuvre de la conformité

- Mettez les **mentions d'informations nécessaires** sur vos sites internet, Facebook, formulaires en fonction des finalités identifiées et les droits de personnes concernées et auprès de qui exercer ce droit ;
- **Revisitez vos formulaires d'inscription**, entre autres, avec notamment **le recueil du consentement** des personnes concernées ;
- **Identifiez les traitements nécessitant une étude d'impact** (dans un deuxième temps), priorisez le registre des traitements) ;
- **Adaptez vos contrats avec vos sous-traitants** en incluant les clauses RGPD (en cas de refus de celui-ci, vous pouvez dénoncer le contrat) ;
- **Documentez les processus de sécurisation des données** (modalités d'accès aux données, qui, à quoi, quand, sauvegardes, cryptage, etc.) ;
- **Documentez le processus de demande d'exercice du droit des personnes concernées ;**
- **Réalisez des audits annuels documentés**

La mise en œuvre de la conformité

• **Prendre en compte le RGPD dans l'évolution de vos missions associatives avant de mettre en place le traitement**

– Définir en amont les données nécessaires et l'impact potentiel sur la vie personnelle en cas de divulgation des données : **« Privacy by Design »** et l'**« Accountability »** ;

– Si besoin, réaliser **une étude d'impact** (AIPD ou PIA) qui doit être validée par le responsable du traitement ;

– Définir les mesures de sécurité à mettre en œuvre autour du traitement ;

– Gérer les relations avec les sous-traitants potentiels en vue de définir un des processus de gestion et choisir une solution adaptée aux besoins et aux contraintes RGPD ;

– S'appuyer sur le DPD pour vous conseiller sur la démarche à suivre avec son rôle de conseil, un regard extérieur et bien souvent des partages d'expériences similaires et des cas de jurisprudence liés au domaine concerné.

RGPD : source de progrès

- **La mise en conformité avec le RGPD permet de :**

  – Réaliser un audit des traitements de la structure et partager une vison globale et transversale du fonctionnement de la structure ;

  – Disposer d'un registre des traitements et des activités ;

  – Revisiter et éventuellement adapter des process de gestion du « On a toujours fait comme ça ! » en se reposant les questions inhérentes au fonctionnement de la structure ;

  – Faire le tri dans ses données et ses fichiers !

  – Se poser les questions nécessaires avant la mise en œuvre d'un nouveau traitement de données à caractère personnel.

Constatations et sanctions

- Constatations :
  - Sur contrôle aléatoire de la CNIL (première chose contrôlée : votre site internet, accessible en ligne!), puis le reste !
  - Le contrôle porte sur l'ensemble du processus de gestion des traitements (informatisés ou non) ainsi que sur la gestion humaine des dossiers
- Les délais de prévenance sont très courts (quelques jours)
  - Sur dénonciation par un tiers auprès de la CNIL
  - Sur constat de manquements au RGPD ou à la loi Informatique & Libertés

Constatations et sanctions

- Les sanctions sont proportionnées aux infractions constatées ;
- Les sanctions peuvent être civiles ou pénales

Infraction	Sanctions
Non-respect des obligations incombant au responsable du traitement	Amende de 10 000 000 € ou 2 % du chiffre d'affaires mondial
Non-respect des obligations incombant au sous-traitant	
Non-respect des exigences du RGPD imposées à l'organisme de certification et à l'organisme de suivi des codes de conduite	
Non-respect de l'obligation de consentement	Amende de 20 millions d'euros ou 4 % du chiffre d'affaires mondial
Non-respect des droits des personnes concernées	
Non-respect de la mise en place de certaines mesures spécifiques relatives au RGPD ou d'une injonction à l'ordre prononcée par la CNIL	

Constatations et sanctions

Plus d'informations : C'est ici

.Quelques exemples :

– Site Internet d'une association (Recettes : environ 9M€ en 2017) Développement de la langue française proposant des cours de français

Motifs de la décision

« la gravité du manquement est caractérisée, notamment au regard du caractère élémentaire de l'incident de sécurité constitué par l'absence de mesures d'authentification des personnes accédant aux documents et par le caractère prévisible des adresses URL permettant de les télécharger »

« Violation des données caractérisée comportant nom, prénom et adresse » chez le sous-traitant. Données non sensibles

Sanction

- de prononcer à l'encontre de l'association X une sanction pécuniaire d'un montant de trente mille (30.000) euros ;
- de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

DATE	NOM OU TYPE D'ORGANISME	MANQUEMENTS PRINCIPAUX / THÈME	DÉCISION ADOPTÉE
21/01/2019	MOTEUR DE RECHERCHE	Manque de transparence, information insatisfaisante et absence de consentement valable	Sanction pécuniaire de 50 000 000 euros
31/01/2019	MOTEUR DE RECHERCHE	Déréférencement	Abandon des poursuites
31/01/2019	SOCIÉTÉ DE GESTION IMMOBILIÈRE	Sécurité et durées de conservation des données personnelles	Abandon des poursuites
31/01/2019	ÉTABLISSEMENT PUBLIC NATIONAL A CARACTÈRE ADMINISTRATIF	Défaut de sécurité des données personnelles	Injonctions sous astreintes
28/05/2019	SOCIÉTÉ DE GESTION IMMOBILIÈRE	Défaut de sécurité des données personnelles et non-respect des durées de conservation	Sanction pécuniaire de 400 000 euros
13/06/2019	SOCIÉTÉ DE TRADUCTION DE DOCUMENTS	Données non adéquates et excessives, non pertinence, information insatisfaisante, défaut de sécurité des données personnelles Vidéosurveillance	Sanction pécuniaire de 20 000 euros et injonction sous astreinte
18/07/2019	SOCIÉTÉ INTERMÉDIAIRE EN ASSURANCE	Défaut de sécurité des données personnelles	Sanction pécuniaire de 180 000 euros
10/10/2019	SOCIÉTÉ DE PHOTOGRAPHIES LIÉES À LA PETITE ENFANCE	Non-respect du droit d'accès, non-respect du droit à l'effacement, défaut de sécurité et de confidentialité des données	Sanction pécuniaire et injonction sous astreinte
21/11/2019	SOCIETE D'INSTALLATION D'EQUIPEMENTS D'ISOLATION	Non adéquation, non pertinence et caractère excessif des données, défaut d'information des personnes, non-respect du droit d'opposition, non coopération avec l'autorité de contrôle, transfert non encadré de données hors de l'UE	Sanction pécuniaire de 500 000 euros et injonction sous astreinte
30/12/2019	SOCIETE D'AIDE A DOMICILE DES PERSONNES AGEES ET HANDICAPEES	Manquement au principe de limitation de la durée de conservation, défaut d'information des personnes, manquement à l'obligation d'assurer la sécurité des données traitées par un sous-traitant	Sanction pécuniaire et injonction sous astreinte

Quelques liens utiles

- CNIL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- ANSSI : https://www.ssi.gouv.fr/
- https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles
- Legalplace : https://www.legalplace.fr/
- Protection des données : Adoptez les 6 bons réflexes – cliquez-ici
- Il existe des applications mobiles permettant de télécharger le RGPD

Le site de la CNIL

Informez-vous et formez vous

Accédez au MOOC de la CNIL : https://atelier-rgpd.cnil.fr/#

Sensibilisation au RGPD

Merci pour votre attention.

Annexe : le droit des personnes

- le droit à l'oubli: selon l'article 17 du RGPD, toute personne concernée par la collecte et le traitement de données peut demander l'effacement de ses données ;

- le droit à la portabilité: la personne concernée peut demander à récupérer l'ensemble de ses données collectées pour les stocker à titre personnel ou les donner à un autre organisme ;

- le droit de rectification: la personne concernée a la possibilité de demander un rectificatif des données erronées dans les meilleurs délais ;

- le droit d'opposition: pour diverses raisons, la personne concernée peut s'opposer au traitement des données la concernant ;

- le droit à la limitation du traitement: la personne concernée est en droit d'interdire au responsable d'utiliser certaines données ;

- le droit d'accès: la personne concernée peut demander d'accéder aux informations la concernant. Elle peut également demander la confirmation que ses données sont ou ne sont pas traitées. L'association dispose d'un mois pour répondre à la demande de la personne concernée.

< Retour au diaporama >

Annexe : L'analyse d'impact

- Liste des traitements pour lesquels l'analyse d'impact est obligatoire :
  https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf

- Liste des traitements pour lesquels l'analyse d'impact n'est pas obligatoire :
  https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf

- Un logiciel est mis à disposition par la CNIL pour vous guider : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

< Retour au diaporama >

FÉDÉRATION CÔTES D'ARMOR
la ligue de l'enseignement
un avenir par l'éducation populaire