Missions Obligatoires

Engagement & Mutualisation

RGPD

Règlement Général sur la Protection des Données

Service RGPD

18 septembre 2023

Missions Facultatives

Innovation & Accompagnement

Sommaire

Première partie

Les notions clés

Qu’est-ce que le RGPD ?

Le responsable de traitement

Le responsable de traitement est la personne morale incarnée par son représentant légal

Obligation

Mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer […] la conformité au règlement
Article 24

Les données personnelles

« Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable »

Données directes

Nom, prénom, adresse postale, numéro de téléphone, date et lieu de naissance, etc.

Pièces justificatives

Carte d'identité, passeport, attestation de domicile, carte vitale, etc.

Données du foyer

Représentants légaux, autres enfants du foyer etc.

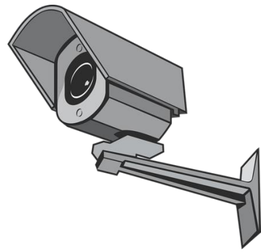
Données indirectes

Données permettant d'identifier une personne indirectement, par recoupement ou échantillonnage

Données sensibles

COLLECTE INTERDITE PAR DEFAUT

- *Origine raciale ou ethnique*
- *Opinions politiques*
- *Convictions religieuses ou philosophiques*
- *Appartenance syndicale*
- *Données génétiques*
- *Données biométriques*
- *Données concernant la santé*
- *Données concernant la vie / l'orientation sexuelle*
- *Numéro de sécurité sociale*



Enregistrements

Vidéos, photos, enregistrement de voix, bande son, etc.

Le traitement de données

« Toute opération ou tout ensemble d'opérations, effectué ou non à l'aide de procédés automatisés, et appliqué à des données à caractère personnel. »

Ces opérations peuvent être :

- la collecte
- l'enregistrement
- l'organisation
- la conservation
- l'adaptation ou la modification
- l'extraction
- la consultation
- l'utilisation
- la communication par transmission
- la diffusion ou toute autre forme de mise à disposition,
- le rapprochement ou l'interconnexion
- l'effacement ou la destruction

Les personnes concernées

Il convient d'identifier avec **précision** les « personnes concernées » par un traitement de données et de définir si elles sont qualifiables de « **personnes vulnérables** »

Dans cette catégorie se trouvent : les mineurs, les agents (dans le cadre de l'exercice de leurs fonctions), les usagers en situation de handicap ou de perte d'autonomie significative, les usagers de plus 65 ans et de manière générale toute personne présentant des difficultés sociales ou d'autre nature.

A NOTER : la présence de données concernant des personnes vulnérables augmente le niveau de risques aux yeux de la CNIL et il convient alors d'apporter des mesures de sécurité supplémentaires

Les personnes concernées (non vulnérables) sont: les usagers, les administrés, les partenaires, etc.

Le registre des traitements

Un registre des traitements est un document qui comprend un descriptif exhaustif de l'ensemble des traitements de données mis en œuvre

Il s'agit d'un document vivant qu'il convient de mettre à jour « en temps réel »

- Liste exhaustive des **finalités** ;
- La **base juridique** du traitement ;
- Liste exhaustive des **données** et des pièces justificatives ;
- Liste exhaustive des **données sensibles**, le cas échéant ;
- Les **personnes concernées** par le traitement ;
- Les **destinataires** des données ;
- Les **sous-traitants**, le cas échéant ;
- Les mesures de **sécurité ;**
- Les **logiciels**, le cas échéant ;
- Les **durées de conservation ;**
- La **forme** des données (papier et/ou numérique) ;

Deuxième partie

Les six principes du RGPD

Les six principes du RGPD

Le Règlement Général sur la Protection des Données (RGPD) pose **six principes** de protection des données que les collectivités doivent suivre lors de la collecte, du traitement et du stockage des données personnelles des **administrés**, des **agents** et des **élus**.

Le responsable du traitement des données est chargé de faire respecter ces principes et doit pouvoir **démontrer la conformité des pratiques** de la collectivité.

Ces principes doivent être appliqués pour tous les traitements, qu'ils soient antérieurs à l'entrée en vigueur du RGPD ou non.

- **Licéité**
- **Finalité**
- **Minimisation**
- **Conservation**
- **Sécurité**
- **Droits des personnes**

Les six principes du RGPD

Le principe de liceité

Pour pouvoir être mis en œuvre, un traitement de données personnelles doit se fonder sur l'une des « bases juridiques » suivantes, listées à l'article 6 du RGPD:

- le **consentement** ;
- le **contrat** ;
- l'**obligation légale** ;
- la **mission d'intérêt public** ;
- l'**intérêt légitime** ;
- la sauvegarde des intérêts vitaux (ne concerne que très rarement les collectivités territoriales).

Les six principes du RGPD

Le principe de finalité

L'article 5 du RGPD prévoit que les données personnelles doivent être collectées :

- pour des finalités **déterminées** : on ne traite donc pas sans but précis, on ne traite pas « au cas où » ;
- **explicites** : il convient d'être transparent sur les traitements que l'on met en œuvre et les raisons pour lesquelles on les met en œuvre ;
- **légitimes** : cela rejoint le principe de licéité ;
- et **ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités** : quand je récolte mes données pour atteindre un objectif A, je ne peux pas m'en servir par la suite pour atteindre un objectif B. Ou alors je demande le consentement préalable des personnes concernées.

Les six principes du RGPD

Le principe de minimisation

L'article 5 du RGPD précise que les données personnelles doivent être **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités** pour lesquelles elles sont traitées.

Une fois l'objectif, la finalité du traitement de données et la base juridique déterminés, seules les données strictement nécessaires pour atteindre cet objectif peuvent être collectées.

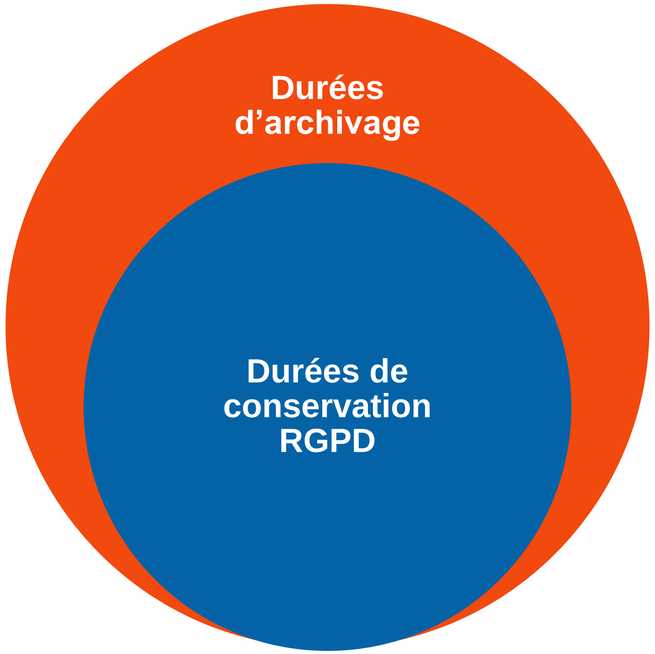
Cela implique parfois de remettre en question ce qui est utile et ce qui ne l'est pas.

Notamment, il est nécessaire de porter une attention particulière à certaines données que l'on recueille par le biais de formulaires par habitude, ou « au cas où », aux données facultatives (qui donc ne seraient pas vraiment indispensables au traitement), et aux champs libres qui peuvent constituer des zones « à risque » dans lesquelles des données peuvent apparaitre sans qu'on les ait demandées mais dont on aura malgré tout la responsabilité.

Une fois que les données sont collectées, le traitement de données est enclenché.

Les six principes du RGPD

Le principe de conservation



Article 5 du RGPD

Les données personnelles doivent être **conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.**

Durées de conservation RGPD : chaque donnée personnelle doit être conservée de façon limitée en fonction des finalités du traitement.

➔ Cela concerne uniquement la base active. Une suppression de données au sein de la base active ne signifie pas élimination de la donnée mais transfert de la donnée vers une base archive.

Durées d'archivage : obligation légale, fixées par un texte de loi, non impactées par le RGPD.

72 heures
pour notifier la CNIL

Les six principes du RGPD

Le principe de sécurité

Article 5 du RGPD *: Les données personnelles doivent être traitées de façon à garantir une sécurité appropriée de celles-ci, 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.*

Il est donc nécessaire de mettre en place des mesures de sécurité de nature à garantir :

- **l'intégrité des données personnelles;**
- **leur confidentialité.**

L'idée est de se prémunir contre une éventuelle **violation de données**

Exemples: piratage informatique, vol ou perte de documents ou de matériel, intrusion dans les locaux, accès à un poste informatique par une personne non autorisée…

Licéité

Finalité

Minimisation

Conservation

Sécurité

Droits des personnes

Les six principes du RGPD

Les droits des personnes

Droit à l'information

Pour être loyale et licite, la collecte de données personnelles doit s'accompagner d'une **information claire et précise** des personnes sur :

- l'identité du responsable du traitement ;
- la finalité du traitement ;
- le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse;
- les destinataires des données ;
- leurs droits ;
- les éventuels transferts de données vers des pays hors UE, etc.

L'information doit être **préalable à la collecte des données**, et le support varie en fonctions des caractéristiques du fichier (panneau d'information pour la vidéosurveillance, mentions d'information sur un formulaire, etc.).

Il conviendra, à terme, de modifier l'ensemble des documents qui vous utilisez pour collecter ou traiter les données afin d'y inclure des **mentions d'information**.

Les six principes du RGPD

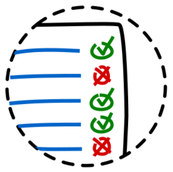
Les droits des personnes

1 mois
pour répondre à la demande

Droit d'accès
Permet d'accéder à l'ensemble des informations la concernant, en connaître l'origine et en obtenir la copie.

Droit à l'effacement
Permet d'obtenir l'effacement de données la concernant (sauf obligation légale)

Droit d'opposition
Permet de s'opposer à ce que ses données personnelles fassent l'objet d'un traitement (sauf obligation légale)



Droit à la limitation
A l'occasion de l'exercice du droit de rectification ou d'opposition, permet demander le gel de l'utilisation de ses données.
Les données ne devront plus être utilisées, mais devront tout de même être conservées.

Droit de rectification
Permet de demander à ce que ses données personnelles faisant l'objet d'un traitement soient corrigées ou complétées.
Le cas échéant, le responsable de traitement doit obligatoirement communiquer aux autres destinataires les rectifications apportées.

Droit à la portabilité
Permet de récupérer une partie de ses données personnelles en vue d'une réutilisation personnelle ou d'une transmission à un autre organisme.
(sauf fichiers papiers)

Attention : les droits varient en fonction de la base juridique du traitement

Troisième partie

Les obligations du responsable de traitement

Les obligations du responsable de traitement

Introduction

Le RGPD impose des « **exigences** » au responsable de traitement qui doivent se répercuter sur l'ensemble des services afin d'obtenir une **uniformité de la démarche**

Ces exigences seront plus ou moins ancrées dans les services en fonction du volume et de la nature des données traitées

- **Accountability**
- **Analyse d'impact**
- **Privacy by design**
- **Registre des traitements**
- **Violation de données**
- **Durée de conservation**
- **Délégué à la protection des données**

Les obligations du responsable de traitement

L'accountability

Ce concept est **LE point central** de la réforme conduite par le RGPD

Il prévoit pour le responsable de traitement une obligation de « rendre des comptes » sur les mesures mises en œuvre pour satisfaire aux dispositions des textes,

L'*accountability* opère le passage d'une logique de conformité basée sur l'accomplissement de formalités auprès de la CNIL à une démarche de conformité qui repose sur la mise en place de la démarche de façon préventive et exclusive,

Concrètement: l'anticipation des études d'impact, la mise en place et le suivi des procédures internes, la gestion des plaintes, les audits internes, la gestion des notifications de violations de données, la sensibilisation récurrente des agents, l'uniformisation des processus et des méthodes de travail.

Accountability

Analyse d'impact

Privacy by design

Registre des traitements

Violation de données

Durée de conservation

Délégué à la protection des données

Les obligations du responsable de traitement

L'analyse d'impact

Il est nécessaire, pour les traitements présentant des risques particuliers pour les droits et libertés des personnes concernées, d'établir une analyse d'impact

(ancienne déclaration CNIL)

Cette analyse repose sur 2 piliers :

1 → une évaluation du système de traitement actuellement mis en œuvre par votre collectivité (finalités, durée de conservation des données, droits des personnes…) ;

2 → une étude de risques sur la sécurité des données (abus, accès aux données personnelles, disparition des données…).

Les obligations du responsable de traitement

L'analyse d'impact

Le texte prévoit une liste de neuf critères d'analyse. Un traitement qui réunit au moins deux des neuf critères doit faire l'objet d'une AIPD :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ou données à caractère hautement personnel ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Validité de 3 ans

Accountability

Analyse d'impact

Privacy by design

Registre des traitements

Violation de données

Durée de conservation

Délégué à la protection des données

Les obligations du responsable de traitement

Le privacy by design

Il consiste à intégrer la dimension de la vie privée dès le stade de la conception du traitement et à mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données.

Concrètement

Application des **six principes** du RGPD et respect des **obligations** du responsable de traitement.

Le Privacy by Design est le pan « prévention » de toute démarche qualité

Les obligations du responsable de traitement

Le registre des traitements

La tenue du registre des traitements est une **obligation légale**.

Il doit être:

- l'exacte vérité des pratiques mises en œuvre (collectives et individuelles) ;
- accessible et compréhensible ;
- maîtrisé et connu par l'ensemble des agents.

Au-delà du RGPD, il est un outil transversal de compréhension des processus.

Les obligations du responsable de traitement

Les violations de données

Cette obligation implique :

1 → de **déterminer** si la violation est susceptible d'engendrer un risque « élevé » pour les personnes concernées ;

2 → de **tenir** un registre des violations de données.

Notification de la violation de données en fonction du niveau de risque			
La violation engendre:	Inscription dans le « registre des violations »	Notification à la CNIL dans un délai maximal de 72h	Informations des personnes concernées
Aucun risque	Oui	Non	Non
Un risque	Oui	Oui	Non
Un risque élevé	Oui	Oui	Oui

Les obligations du responsable de traitement

Les durées de conservation

Les durées de conservation doivent être déterminées et limitées par le responsable de traitement à ce qui est nécessaire à la finalité.

Au-delà de ces durées, les données doivent être :

Détruites

Anonymisées

Archivées

→ Utilisation des circulaires du Service Interministériel des Archives.

Les obligations du responsable de traitement

Le délégué à la protection des données

Le Délégué à la Protection des Données succède au correspondant informatique et libertés (CIL).

Sa désignation est obligatoire.

Ses missions consistent à :

- informer et conseiller le responsable de traitement ;
- contrôler le respect du RGPD ;
- conseiller sur la réalisation d'analyses d'impact ;
- coopérer avec l'autorité de contrôle.

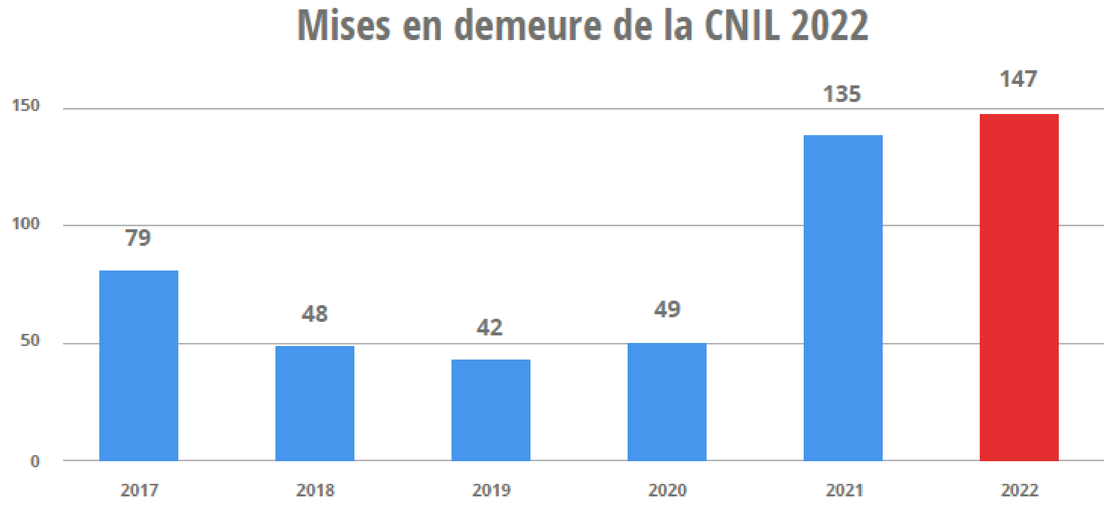
Quatrième partie

Les sanctions et les bonnes pratiques

Des risques pour les collectivités…

2022 : une année record pour la CNIL

- **Une forte augmentation des mises en demeure**
- **2021 : 18 sanctions financières - 214 millions € (+55%)**
- **2022 : 21 sanctions financières - 101 millions €**
- **Sanction de 22 communes n'ayant pas désigné un DPD**



Manquements les plus fréquents :

- ✓ *Défaut d'information des personnes*
- ✓ *Durées de conservation excessives*
- ✓ *Sécurisation insuffisante*
- ✓ *Mauvaise gestion des cookies*
- ✓ *Surveillance vidéo, caméras police-municipale*

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

Sur la décision de sa présidence, la CNIL peut contrôler tout organisme traitant des données à caractère personnel dès lors qu'il dispose d'un établissement en France ou que le traitement concerne des personnes physiques résidant en France.

Les collectivités peuvent faire l'objet d'un contrôle pour l'une (ou plusieurs) des raisons suivantes :

- mise en œuvre de traitements inscrits dans le **programme annuel** de la CNIL ;
- à la suite d'une **plainte** individuelle ou collective déposée auprès de la CNIL ;
- lorsque la CNIL reçoit un **signalement** de la part d'autres autorités ;
- lorsque l'attention des **médias** s'est portée sur l'organisme ;
- à la suite d'un contrôle dans les locaux d'un **sous-traitant** ou d'un co-responsable de traitement ;
- dans le cadre du contrôle des dispositifs de **vidéo-protection et de vidéo-surveillance.**

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

La CNIL publie tous les ans un programme indiquant les secteurs et les activités de traitement de données pour lesquels des contrôles seront menés l'année suivante

Exemples de thématiques (2023)

L'ensemble des traitements RH

RECRUTEMENT DU PERSONNEL

GESTION DES SERVICES DE STATIONNEMENT

COOKIES ET AUTRES TRACEURS

Site internet, réseaux sociaux, etc

Et des personnes vulnérables

DONNEES DES MINEURS

SECURITE DES DONNEES DE SANTE

Comprenant le volet social

SERVICES DE GEOLOCALISATION

Y compris la surveillance des bâtiments et des installations

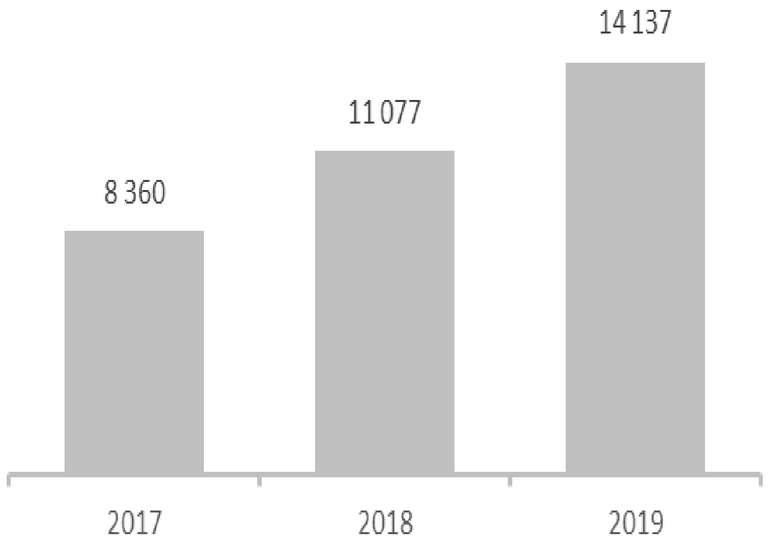
- Traitements inscrits dans le programme annuel
- Plainte individuelle ou collective
- Signalement d'une autre autorité
- Attention des médias
- Contrôle d'un sous-traitant
- Dispositifs de vidéo-protection et de vidéo-surveillance

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

Les plaintes sont en forte hausse ces dernières années

Plus de 40 % des contrôles diligentés par la CNIL



Nombre de contrôles par an

Exemple:

La CNIL a prononcé une sanction pécuniaire (50 millions d'euros) à l'encontre d'un éditeur de système d'exploitation à la suite des plaintes collectives déposées par deux associations, regroupant les réclamations de 9 974 personnes concernées.

Manquement :

Non respect du droit à l'information et de l'accessibilité aux droits des personnes

Traitements inscrits dans le programme annuel

Plainte individuelle ou collective

Signalement d'une autre autorité

Attention des médias

Contrôle d'un sous-traitant

Dispositifs de vidéo-protection et de vidéo-surveillance

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

La CNIL peut diligenter un contrôle après avoir

obtenu des informations de la part d'une autre autorité

Exemple:

La CNIL a été informée par le client d'une société en assurance que les données d'autres clients étaient accessibles sans procédure d'authentification aux espaces personnels des clients sur le site web de la société.

Manquement:

Non respect du principe de sécurité devant garantir l'intégrité et la confidentialité des données.

- Traitements inscrits dans le programme annuel
- Plainte individuelle ou collective
- Signalement d'une autre autorité
- Attention des médias
- Contrôle d'un sous-traitant
- Dispositifs de vidéo-protection et de vidéo-surveillance

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

La CNIL peut décider de faire un contrôle lorsque des problématiques et enjeux relatifs à la protection des données à caractère personnel sont évoqués par les médias

Exemple :

Après la publication de plusieurs articles de presse révélant l'utilisation de drones équipés de caméras par la police et la gendarmerie pour surveiller le respect du confinement, la Présidente de la CNIL a décidé de diligenter un contrôle sur pièces, suivi par un contrôle sur place. A la suite de ces vérifications, une procédure de sanction a été engagée et la formation restreinte de la CNIL a prononcé un rappel à l'ordre ainsi qu'une injonction à l'encontre du ministère de l'intérieur.

Manquement :

Non respect du principe de finalité

- Traitements inscrits dans le programme annuel
- Plainte individuelle ou collective
- Signalement d'une autre autorité
- Attention des médias
- Contrôle d'un sous-traitant
- Dispositifs de vidéo-protection et de vidéo-surveillance

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

La CNIL peut effectuer un contrôle de la conformité d'un sous-traitant, d'un prestataire ou d'un co-responsable de traitement.

Cela peut être le cas, par exemple, lorsqu'une collectivité initialement contrôlée n'est pas, après les premières investigations, le responsable de traitement de l'activité visée par la CNIL.

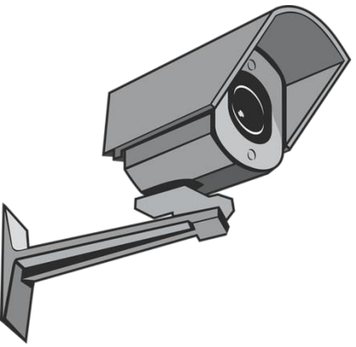
Un tel scénario peut également se produire dans le cadre de relations contractuelles. A la suite d'un contrôle dans une collectivité, la CNIL peut procéder à un contrôle auprès du prestataire auquel la collectivité a confié tout ou partie de ses activités de traitement, ou inversement.

C'est également le cas en cas de délégation de service.

Les contrôles de la CNIL

Pourquoi ma collectivité est-elle contrôlée ?

La CNIL est compétente pour contrôler les conditions de mise en œuvre et d'utilisation des systèmes de vidéo-protection et de vidéo-surveillance dans des lieux ouverts au public



<u>Principaux manquements constatés :</u>

Non respect du principe de finalité

Défaut d'information aux personnes concernées

Non-respect et/ou atteinte de/à la vie privée

Traitements inscrits dans le programme annuel

Plainte individuelle ou collective

Signalement d'une autre autorité

Attention des médias

Contrôle d'un sous-traitant

Dispositifs de vidéo-protection et de vidéo-surveillance

Les contrôles de la CNIL

Quels sont les types de contrôles ?

Il existe quatre types de contrôles : sur place, sur pièces, sur audition et en ligne

- Deux agents habilités seront désignés (un juriste et un auditeur des systèmes d'information).
- Quelle que soit la forme qu'il prenne, l'objectif d'un contrôle est de vérifier la conformité d'un traitement mis en œuvre par une collectivité.
- A ce titre, les agents de la CNIL peuvent notamment demander la communication de toute information ou de tout renseignement qu'ils estiment utiles.

Les contrôles de la CNIL

Comment anticiper un contrôle?

Tout contrôle emporte des risques financiers, juridiques, opérationnels ou encore de réputation.

Ces risques existent également pour les collectivités qui semblent, au premier abord, en conformité avec le cadre réglementaire. La non-conformité peut être identifiée à la fin de la procédure de contrôle et ainsi remettre en cause la continuité des activités de la collectivité.

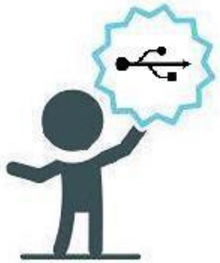
Anticiper un contrôle participe plus généralement à une gestion des risques.

A ce titre, les collectivités peuvent mettre en place les actions suivantes :

- cartographier les actions de non-conformités et suivre leur mise en œuvre ;
- préparer les documents généralement demandés par la CNIL ;
- mettre en place une procédure de gestion des contrôles ;
- sensibiliser et former les agents.

Les bonnes pratiques informatiques et protection des données

Je verrouille ma session dès que je quitte mon poste de travail en utilisant la combinaison de touches ctrl+alt+suppr ou windows+L.



Je n'utilise jamais de clé usb ou de disque dur externe personnel.

J'utilise exclusivement les espaces de stockage prévus et ne laisse rien en local.

Je fais attention au contenu des mes échanges par courriels avec l'extérieur.

Ceux-ci ont la même valeur juridique que les courriers.

Je signale sans délai tout risque sur les données à mon responsable et au DPD.
Exemples : perte de document, envoi d'informations au mauvais destinataire, mail suspect, etc.

Les bonnes pratiques informatiques et protection des données

Je protège la confidentialité des données auxquelles j'ai accès et ne les communique pas à des tiers.
Je range mes documents papiers dans des armoires ou des caissons fermés.

Je recueille, utilise et ne conserve que les données qui sont indispensables pour mon travail.

Je supprime mes fichiers temporaires et mes brouillons.

J'utilise uniquement mes identifiants personnels et veille à ce que personne n'en prenne connaissance.

Je ne les transmets ni à mes collègues, ni à mes responsables.

J'applique l'ensemble de ces règles pendant mes déplacements et en télétravail.

Cinquième partie

L’accompagnement de la mission RGPD mutualisée

L’accompagnement de la mission RGPD mutualisée

Un socle de conformité :

- Accès à un espace RGPD enrichi : pilotage de votre conformité et documentation probatoire ;
- Nouvelles communications, informations, sensibilisations ;
- Accompagnement complet de DPD : réponses à vos questions, analyses de cas concrets, demandes d’exercice de droits**, violation de données, accompagnement à la réalisation d’une étude d’impact, relations avec la CNIL (contrôle, plainte).**

De manière facultative et sur demande, des prestations supplémentaires :

- **Réalisation d’un diagnostic RGPD au sein de votre collectivité** : sensibilisations agents et élus, entretien avec les agents, registre des traitements, rapport, plan d’actions, suivi périodique ;
- **Préparation à un contrôle CNIL** : formation des agents, établissement d’une procédure, simulation d’audit, livrable de préconisations ;
- **Accompagnement du référent RGPD** : formation, appui à la mise en conformité, suivis réguliers.

Merci pour votre attention !