TD1 : La loi « informatique et libertés » et introduction au RGPD

==> cnil.fr

1 – Rappelez la composition et les 4 principales missions de la **CNIL**

https://www.cnil.fr/fr/statut-et-organisation-de-la-cnil

https://www.cnil.fr/fr/les-missions-de-la-cnil

Le CNIL est composé de 18 membres, dont 6 représentants de hautes juridictions, 5 personnalités qualifiées, 4 parlementaire, 2 membres du conseil économique, social et environnement et 1 membre de la commission d'accès aux documents administratifs.

Et les 4 principales missions sont :

Mission 1 – Informer, protéger les droits -> Informer : La CNIL est investie d'une mission générale d'information des personnes des droits et répond aux demandes des particuliers et des professionnels : 161 475 appels reçus au standard, en 2021 16 898 requêtes reçues par voie électronique et 10.8 millions de visites sur les sites web. Protéger : La CNIL veille à ce que les citoyens accèdent efficacement aux données contenues dans les traitements les concernant : 14 143 plaintes qui ont conduit à : 5848 réponses rapides et 8 295 étude plus approfondie, 5 329 demandes valables de droit d'accès indirect.

Mission 2 – Accompagner la conformité / conseiller -> Accompagner : Afin d'aider les organismes privés et publics à se mettre en conformité avec le RGPD, la CNIL propose une boîte à outils complète et adaptée en fonction de leur taille et de leurs besoins.: 81 393 Organismes ont désigné un délégué à la protection des données, 29 810 DPO désignés. Conseiller : la CNIL veille à la recherche de solutions permettant aux organismes publics et privés de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens : 22 auditions parlementaires, 576 Autorisation de recherche en santé dont 54 sur la COVID-19, 154 autres délibérations dont 121 avis sur des projets de texte.

Mission 3 – Anticiper et innover -> Dans le cadre de son activité d'innovation et de prospective, la CNIL s'intéresse aux signaux faibles et aux sujets émergents. Elle participe ainsi à la constitution d'un débat de société sur les enjeux éthiques des données.

Mission 4 – Contrôler et sanctionner -> Le Contrôle : Le contrôle à posteriori constitue un moyen privilégié d'intervention auprès des responsables de traitement de données personnelles L'Avertissement : la présidente de la CNIL peut avertir un organisme que le traitement de données qu'il envisage, à un stade où celui-ci n'est pas encore opérationnel, est susceptible de méconnaître les textes applicables. Mise en demeure : La Présidente de la CNIL a la possibilité de mettre en demeure des organismes qui ne respectent pas des dispositions du RGPD ou de la loi de se mettre

en conformité dans un délai imparti : 135 mises en demeure dont 2 publiques. La Procédure de Sanction de la CNIL : A l'issue de contrôle ou de plaintes, en cas de méconnaissance des dispositions du RGPD ou de la loi de la part des responsables de traitement et des sous-traitants, la formation restreinte de la CNIL peut prononcer des sanctions à l'égard des responsables de traitements qui ne respecteraient pas ces textes.

2 – Définissez brièvement les 8 différents droits subjectifs d'une personne fichée (CNIL + RGPD) :

Droit d'accès direct, droit d'accès indirect, droit d'opposition, droit à l'oubli (ou à l'effacement), droit au déréférencement, droit à l'information, droit à la portabilité et droit à la limitation du traitement.

3 – La plainte en ligne et les courriers pour agir : Comment ça marche ?

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

https://www.cnil.fr/modeles/courrier

Tout d'abord il faut sélectionner un thème :

Ensuite sélectionner son cas :

Préciser où en sont vos démarches :

Ensuite il faut écrire au responsable du site :

Madame, Monsieur,

Des informations me concernant sont actuellement diffusées sur votre site internet sur les pages suivantes :

[urls]

Aussi, en application des articles 21.1 et 17.1.c. du Règlement général sur la protection des données (RGPD), je vous remercie de supprimer les données personnelles suivantes me concernant :

[infos_a_supprimer] .

Je souhaite que ces informations soient supprimées car :

[motif_de_la_suppression]

Je vous remercie également de faire le nécessaire pour que ces pages ne soient plus référencées par les moteurs de recherche (article 17.2 du RGPD).

Vous voudrez bien me faire parvenir votre réponse dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de ma demande (article 12.3 du RGPD).

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Ou sinon si on choisit autre cas :

Sélectionnez un thème

VOTRE THÈME 1 — VOTRE PROBLÈME 2 — VOTRE DÉMARCHE 3

INTERNET | COMMERCE | TRAVAIL | TÉLÉPHONIE

BANQUE ET CRÉDIT | AUTRES CAS

Sélectionnez votre cas

VOTRE THÈME AUTRES CAS 1 — VOTRE PROBLÈME 2 — VOTRE DÉMARCHE 3

AUTRES CAS

Votre problème n'est pas listé parmi les cas de plaintes ? Vous pensez que votre problème concerne un manquement à la loi Informatique et Libertés.

Vérifiez d'abord si une réponse à votre problème existe dans notre service d'aide en ligne.

En cas d'absence de réponse pertinente, vous aurez la possibilité de nous adresser une demande par voie électronique (lien accessible lors de la consultation de l'une de nos FAQ, en bas de page)

On va prendre par exemple dossier médical :

Posez votre question, la CNIL vous répond

Vous recherchez une information ? Les questions les plus fréquemment posées sont recensées ici.
Posez votre question dans l'encadré ci-dessous, notre système vous transmettra les questions-réponses en lien avec votre problématique.

Dossier médical OK

- Accès à mon dossier médical : dans quel délai doit-on me répondre ?
- DMP (dossier médical personnel) et dossier médical : quelle différence ?
- DMP (dossier médical personnel) : qui peut le consulter ?
- DMP (dossier médical personnel) et dossier médical : quelles différences ?
- DMP (dossier médical personnel) : qui peut le consulter ?
- Comment accéder à mon dossier médical ?
- Dossier médical : que faire si on me refuse l'accès ?

Comment accéder à mon dossier médical ?

Vous avez le droit de connaître toutes les informations concernant votre santé détenues par un médecin ou par un établissement de santé.

Pour cela, demandez à accéder à ces informations en personne ou par l'intermédiaire du médecin de votre choix.

Vous avez le choix de consulter votre dossier sur place et d'en faire des copies, ou de demander que les documents vous soient adressés par courrier, de préférence avec accusé de réception.

Cas particuliers :

- **patient mineur** : il peut s'opposer à la communication de son dossier médical au(x) titulaire(s) de l'autorité parentale ;
- **patient décédé** : les héritiers d'une personne décédée peuvent, sauf volonté contraire exprimée de son vivant, accéder à certaines informations du dossier médical pour connaître les causes du décès, défendre la mémoire du défunt ou faire valoir leurs droits ;
- **patient en soins psychiatriques sans consentement** : en cas de risques d'une gravité particulière, l'accès au dossier médical peut s'effectuer par l'intermédiaire d'un médecin. Si le patient s'y oppose, la Commission départementale des hospitalisations psychiatriques émet un avis qui s'impose à tous.

> Retour

4 – Quelles sont les autorisations et les interdictions relatives à la mise en place d'un dispositif de vidéosurveillance ? (Travail, commerces, établissements scolaires, voie publique, chez soi, immeubles d'habitation, vidéoprotection)

https://www.cnil.fr/fr/videosurveillance-videoprotection

Au travail :

La vidéosurveillance – vidéoprotection au travail

27 novembre 2019

Les caméras de surveillance sont aujourd'hui largement utilisées sur les lieux de travail. Si ces outils sont légitimes pour assurer la sécurité des biens et des personnes, ils ne peuvent pas conduire à placer les employés sous surveillance constante et permanente. Quelles règles les employeurs doivent-ils respecter ? Quels sont les droits des employés ?

Seules les personnes habilitées par l'employeur, et l'employeur doit définir la durée de conservation des images issues des caméras. Cette durée doit être en lien avec l'objectif poursuivi par les caméras. En principe, cette durée n'excède pas un mois.

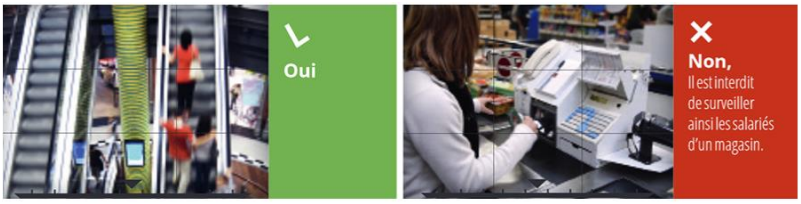
Dans les commerce :

La vidéosurveillance dans les commerces

03 décembre 2019

Les commerçants ont recours à des caméras pour lutter contre les vols de marchandises par les clients ou les employés.

Ces dispositifs sont soumis à différentes règles selon la zone surveillée. Quelles sont ces règles ? Quelles précautions prendre ? Quels sont les droits des personnes filmées ?



Les images enregistrées ne doivent **pas être librement accessibles** à l'ensemble des employés ou des clients. Seuls les responsables de la sécurité, les agents de sécurité ou la direction du magasin doivent pouvoir les visualiser. Le responsable du dispositif doit définir la durée de conservation des images issues des caméras. Cette durée doit être en lien avec l'objectif poursuivi par les caméras. En principe, cette durée n'excède pas un mois.

Dans les établissement scolaire :

La vidéosurveillance – vidéoprotection dans les établissements scolaires

03 décembre 2019

Pour sécuriser les accès et éviter les incidents, des caméras sont installées dans les établissements scolaires pour filmer les couloirs, les halls d'entrées, mais aussi la rue. Ces dispositifs doivent respecter différentes règles afin de ne pas porter atteinte à la vie privée des personnes filmées. Quelles sont ces règles? Quelles précautions prendre ?

Seules les personnes habilitées dans le cadre de leurs fonctions (par exemple : le chef d'établissement), peuvent visionner les images enregistrées. Le responsable du dispositif doit définir la durée de conservation des images issues des caméras.Cette durée doit être en lien avec l'objectif poursuivi par les caméras. En principe, cette durée n'excède pas un mois.

Sur voie publique :

La vidéosurveillance – vidéoprotection sur la voie publique

03 décembre 2019

Le nombre de caméras filmant la voie publique a fortement augmenté ces dernières années, notamment sous l'impulsion des pouvoirs publics, pour lutter contre l'insécurité. Des textes spécifiques encadrent ces dispositifs soumis à une autorisation du préfet. Quelles sont les règles ? Quels sont les droits des personnes filmées ?

Les personnes filmées ont un droit d'accès aux images sur lesquelles elles apparaissent. La durée de conservation des images doit être **proportionnée** et **correspondre à l'objectif pour lequel le système de vidéoprotection est installé**. En règle générale, quelques jours suffisent pour effectuer des vérifications, par exemple à la suite d'un incident.

Les personnes filmées dans un espace public doivent en être informées, au moyen de panneaux affichés en permanence, de façon visible, dans les lieux concernés, et doivent être compréhensibles par tous les publics.

Chez soi :

La vidéosurveillance, vidéoprotection – chez soi

13 décembre 2019

Les particuliers ont régulièrement recours à des caméras pour sécuriser leur domicile, notamment pour lutter contre les cambriolages.

Ces dispositifs doivent toutefois respecter la vie privée des personnes filmées. Quelles précautions prendre lors de l'installation de tels dispositifs ?

Dans les immeubles :

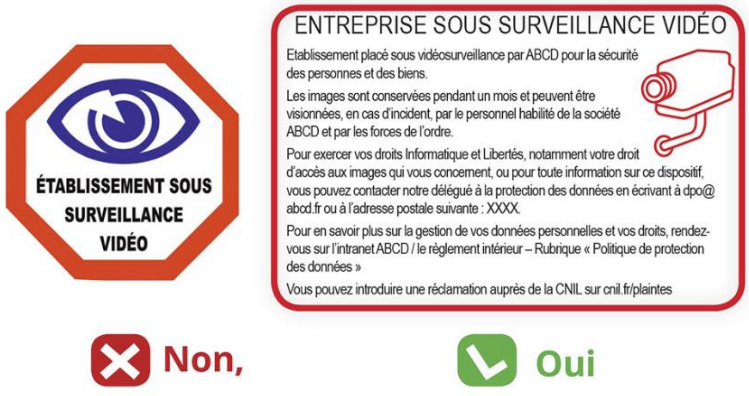
La vidéosurveillance – vidéoprotection dans les immeubles d'habitation

03 décembre 2019

Pour lutter contre les vols ou les dégradations dans les parkings ou les halls d'entrée de plus en plus d'immeubles sont équipés de caméras de vidéosurveillance. Ces dispositifs doivent respecter différentes règles afin de ne pas porter atteinte à la vie privée des personnes. Quelles sont ces règles ? Quelles précautions prendre ? Quels sont les droits des personnes filmées ?

Les dispositifs permettant de visualiser des images en direct ou enregistrées, ne doivent **pas être librement accessibles** à l'ensemble des habitants. La durée de conservation des images ne devrait **pas excéder un mois**. En règle générale, conserver les images quelques jours suffit à effectuer les vérifications nécessaires en cas d'incident, et permet d'enclencher d'éventuelles procédures pénales.

Les personnes filmées dans un espace public doivent être informées, au moyen de panneaux affichés en permanence, de façon visible, dans les lieux concernés, et doivent être compréhensibles par tous les publics.



Vidéoprotection :

Vidéoprotection : quelles sont les dispositions applicables ?

13 décembre 2019

L'entrée en application du « Paquet européen de protection des données personnelles » constitué du règlement général sur la protection des données (RGPD) et de la directive « Police-Justice », transposée en droit français, a modifié le cadre juridique que doivent respecter les responsables de traitement qui envisagent d'installer des systèmes de vidéoprotection soumis aux dispositions du code de la sécurité intérieure.

Quels sont les dispositifs concernés ?

Ce sont les systèmes de vidéoprotection visés par l'article L251-2 du code de la sécurité intérieure (CSI), qui filment la voie publique et les lieux ouverts au public (espaces d'entrée et de sortie du public, zones marchandes, comptoirs, caisses, etc.), à la différence des dispositifs de vidéosurveillance, qui filment des lieux privés ou des lieux de travail non ouverts au public (locaux d'entreprises, de commerces, d'hôtels réservés aux salariés, etc.).

Comment déterminer si le dispositif relève du RGPD ou de la directive « Police-Justice » ?

Pour les responsables de traitement, la difficulté, résultant du droit européen, consiste à déterminer si leur dispositif de vidéoprotection relève du champ du RGPD ou du champ de la directive « Police-Justice ».

La réponse à cette question dépend de l'objectif exact du système de vidéoprotection envisagé.

Ainsi, s'il est mis en œuvre, dans le cadre de leurs missions, par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, il relève des **dispositions transposées de la directive**.

Les finalités prévues par le code de la sécurité intérieure (CSI) entrant dans ce cadre sont les suivantes :

FINALITÉ DU SYSTÈME DE VIDÉOPROTECTION	ARTICLE DU CODE DE LA SÉCURITÉ INTÉRIEURE VISÉ
Protection des bâtiments et installations publics et de leurs abords	L251-2-1°
Constatation des infractions aux règles de la circulation	L251-2-4°
Prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions	L251-2-5°
Respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile	L251-2-10°
Assurer la protection des abords immédiats des bâtiments et installations de commerçants installés dans les lieux particulièrement exposés à des risques d'agression ou de vol	L251-2 dernier alinéa

Dans le cas contraire, le système de vidéoprotection relève du RGPD dès lors qu'il a pour objet l'une des finalités suivantes :

FINALITÉ DU SYSTÈME DE VIDÉOPROTECTION	ARTICLE DU CODE DE LA SÉCURITÉ INTÉRIEURE VISÉ
Régulation des flux de transports	L251-2-3°
Prévention des risques naturels ou technologiques	L251-2-7°
Sécurité des installations accueillant du public dans les parcs d'attraction	L251-2-9°
Assurer la sécurité des personnes et des biens dans des lieux et établissements ouverts au public, lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol	L251-2-12°

Enfin, le système de vidéoprotection relève de la loi « Informatique et Libertés » (hors champ du droit de l'Union européenne) dès lors qu'il a pour objet :

FINALITÉ DU SYSTÈME DE VIDÉOPROTECTION	ARTICLE DU CODE DE LA SÉCURITÉ INTÉRIEURE VISÉ
Sauvegarde des installations utiles à la défense nationale	L251-2-2°
Prévention d'actes de terrorisme (dans les conditions prévues au chapitre III du titre II du livre II du CSI)	L251-2-6°

les mesures à prendre avant d'installer un système de vidéoprotection :

-Faire une demande d'autorisation adressée au préfet territorialement compétent

-Mener une analyse d'impact sur la protection des données (AIPD)

-Informer les personnes susceptibles d'être filmées par un système de vidéoprotection

-Limiter la durée de conservation des images à ce qui est nécessaire au regard de la finalité poursuivie

-Assurer la sécurité des données traitées

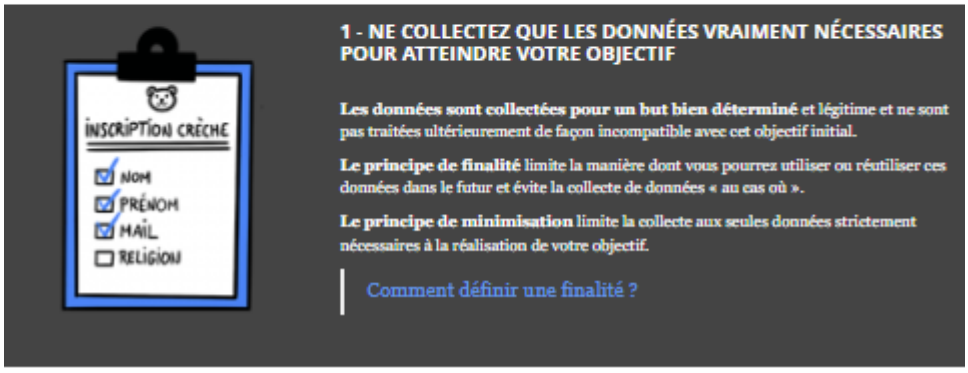
-Répondre aux demandes de droit d'accès

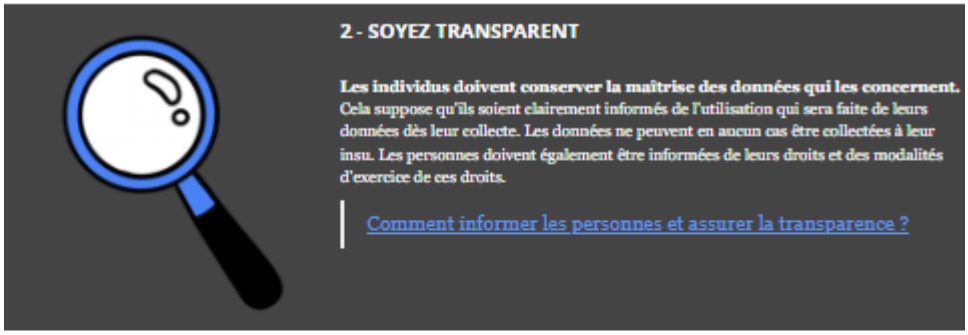
5 – Résumez : « Comprendre le RGPD » : Les 6 bons réflexes et ce qui change (pour les professionnelles, les sous-traitants)

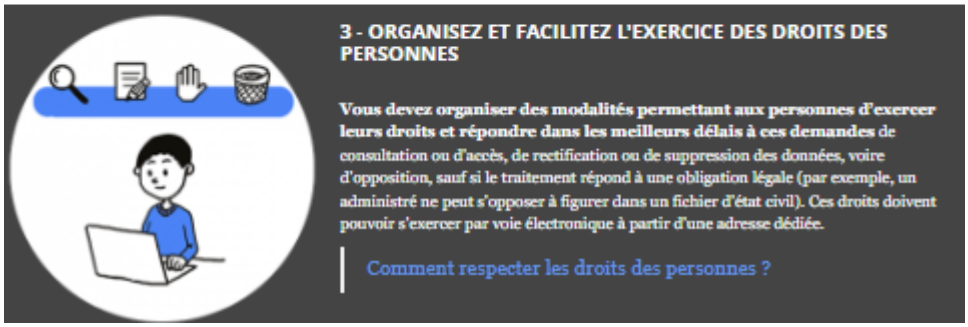
Adopter les six bons réflexes

18 septembre 2019

Ces 6 réflexes reprennent des notions ou principes qui peuvent vous être utiles pour sensibiliser votre entourage professionnel à la protection des données personnelles.







Conformité RGPD : comment informer les personnes et assurer la transparence ?

26 juillet 2019

Le règlement général sur la protection des données (RGPD) impose une information concise, transparente, compréhensible et aisément accessible des personnes concernées. Cette obligation de transparence est définie aux articles 12, 13 et 14 du RGPD. La CNIL fait le point sur les mesures permettant de respecter cette obligation.

Ce contenu a été mis à jour le 26 juillet 2019

Le RGPD impose une information complète et précise. Les modalités de fourniture et de présentation de cette information doivent être adaptées au contexte.

La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.

Pour les responsables de traitement, elle contribue à un traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées.

6 – Qu'est-ce que la biométrie (avec trace et sans trace) ?

– Et quelles sont les conditions de collecte des données biométriques (pour contrôle d'accès sur les lieux de travail et dans les smartphones) ?

https://www.cnil.fr/fr/biometrie

Biométrie

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.).

Sur les lieux de travails :

Le contrôle d'accès biométrique sur les lieux de travail

Les dispositifs biométriques sont strictement encadrés par la loi Informatique et Libertés et par le règlement européen sur la protection des données.

Deux types de dispositifs :

1. Les dispositifs biométriques dont le gabarit est stocké dans l'appareil, sous le seul contrôle du particulier.

De nombreux appareils mobiles intègrent des dispositifs biométriques fonctionnant de manière autonome, dans un environnement totalement cloisonné au sein de l'appareil qui empêche que les données biométriques en elles-mêmes ne soient accessibles à l'extérieur de l'enclave.

Dans ces cas, le gabarit biométrique est enregistré dans l'appareil, dans une sorte de « boîte » hermétique, et ne sort jamais de cette « boîte ».

En pratique, lorsque l'utilisateur s'authentifie, le doigt posé sur le lecteur de l'appareil est comparé avec le gabarit biométrique préalablement enregistré.

Le service ou l'application qui utilise ce mode d'authentification ne reçoit qu'une information sur la réussite ou l'échec de la comparaison entre le doigt présenté et le gabarit.

Dans ces cas, la CNIL considère que les traitements mis en œuvre à l'initiative et sous le seul contrôle de la personne concernée, **peuvent être couverts par l'exemption domestique** inscrite à l'article 2-2-c du RGPD.

2. Les dispositifs biométriques fonctionnant depuis des serveurs distants

Dans d'autres cas, les dispositifs d'authentification basés sur la reconnaissance biométrique fonctionnent en interaction avec des serveurs distants maîtrisés par un organisme tiers, quels qu'il soient.

L'organisme en question (qu'il s'agisse du fournisseur de l'application, de l'appareil, etc.) **doit alors effectuer une analyse d'impact relative à la protection des données (AIPD).** Le traitement de données envisagé est en effet susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées compte tenu notamment de la sensibilité des données traitées et du caractère innovant des technologies employées.

Cette analyse d'impact (AIPD) devra être transmise à la CNIL pour consultation si le niveau de risque résiduel reste élevé.

Les dispositifs d'authentification biométrique pouvant relever de l'exemption domestique

(Article 2 du règlement européen sur la protection des données)

Le recours à un dispositif de reconnaissance biométrique intégrée à un appareil n'est pas soumis aux obligations prévues par le RGPD, dès lors que sont satisfaits les critères suivants :

1. **l'utilisateur utilise ce dispositif à titre privé,** grâce à ses propres données biométriques, pour déverrouiller son téléphone ou pour accéder à des applications qu'il a téléchargées de son propre chef ;
2. **l'utilisateur décide seul d'utiliser l'authentification biométrique** intégrée dans son appareil :
   - Cela **exclut toute authentification biométrique imposée par un employeur**, notamment si l'appareil lui a été fourni dans le cadre de ses activités professionnelles.
   - Cela implique que les fournisseurs d'application **proposent un mode d'authentification alternatif** à la biométrie (par exemple la saisie d'un code), sans contrainte additionnelle. Si le fournisseur d'application ne propose que l'authentification biométrique, le traitement de données correspondant relève de la responsabilité du fournisseur et est soumis aux dispositions du RGPD.
3. le gabarit biométrique est **stocké dans l'appareil,** dans un environnement cloisonné et n'est pas accessible ou transmis à l'extérieur :
   - Cela **exclut** les dispositifs biométriques envoyant le gabarit dans une **base de données distante**.
   - Il **exclut** aussi **toute possibilité d'intervention** d'un organisme extérieur (fournisseur de l'appareil ou d'une application par exemple) sur les données biométriques.
4. le gabarit biométrique est stocké dans l'appareil de manière **chiffrée** à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art ;
5. lors du contrôle d'accès, **seul un jeton** ou une donnée indiquant la réussite ou l'échec de la reconnaissance de la biométrie présentée est transmis.

Les dispositifs fonctionnant dans ces conditions **intègrent par défaut des mécanismes protecteurs de la vie privée :**

- la donnée biométrique ne risque pas d'être récupérée et détournée par un organisme extérieur si elle reste dans un « compartiment » fermé, à l'intérieur de l'appareil, et si cet appareil reste sous le contrôle de son utilisateur.
- le choix de recourir à l'authentification biométrique appartient au principal intéressé et n'est pas lié à une contrainte extérieure.

Les dispositifs biométriques proposés aux particuliers soumis au RGPD

Lorsque le dispositif de reconnaissance biométrique proposée à la personne sur son appareil fonctionne en interaction avec des serveurs distants maîtrisés par un organisme tiers, l'organisme doit respecter les obligations prévues par le RGPD :

- **s'il est le décideur** de la mise en place de l'authentification biométrique dans un contexte donné ;
- **s'il maîtrise en tout ou partie** les moyens de traitement biométriques (par exemple, un lecteur biométrique ou une base permettant de stocker le gabarit).

Pour les smartphones :

Biométrie dans les smartphones

Les mécanismes d'authentification biométriques sur les smartphones se généralisent. La CNIL a établi les conditions dans lesquelles ces traitements de données biométriques sont, ou non, soumis au cadre de protection des données..

Le nouveau cadre règlementaire

L'entrée en application du RGPD le 25 mai 2018 a profondément affecté le cadre juridique existant.

La logique d'autorisation préalable et plus largement celle de formalités administratives a disparu, remplacée par une logique de responsabilisation des acteurs dite d' « accountability ». Cette démarche de conformité dynamique oblige les organismes à s'assurer en interne de la licéité de leurs traitements et des conditions de mise en œuvre avant leur mise en œuvre, et veiller plus globalement au respect de l'ensemble des obligations en matière de protection des données.

Par ailleurs, la nature même des données biométriques a évolué : désormais qualifiées de « données sensibles » par le RGPD, leur traitement devient en principe interdit sauf à s'inscrire dans l'une des exceptions limitativement prévues par le texte.

Sensible à ces évolutions, le législateur français a confié à la Commission une mission nouvelle, qui est celle de concevoir et de publier en concertation avec des organismes représentatifs des acteurs concernés, des règlements type en matière notamment de traitement des données biométriques.

Le règlement type « biométrie sur les lieux de travail » s'inscrit dans la continuité des positions antérieures de la CNIL en la matière. Il précise aux organismes comment encadrer leurs traitements de données biométriques de contrôle d'accès aux locaux, aux applications ou aux outils de travail et revêt un caractère contraignant. Les organismes qui mettent en œuvre ces traitements sont donc tenus de respecter les indications données dans le règlement type.

Comment procéder pour se mettre en conformité ?

Etape 1 - Justifier le besoin d'un dispositif biométrique | Etape 2 - Garantir la maîtrise du gabarit | Etape 3 - Justifier et documenter les choix effectués