

# Le RGPD appliqué au Cabinet Dentaire

dr SALLIOT Adeline -URPS ara

# Naissance du RGPD: les prises de conscience

- ▶ 1973: Projet SAFARI : interconnexion des fichiers d administration
- ▶ 21-03-1974: Le quotidien le monde dévoile ce projet
- ▶ 06-01-1978 Loi dite informatique et libertés avec création d une entité de contrôle indépendante la CNIL
- ▶ 24-10-1995 : Directive européenne
- ▶ 2013: Edward Snowden mettait au jour des centaines de milliers de documents révélant la surveillance de masse jugée « abusive » de son employeur, la National Security Agency (NSA). 7 ans plus tard, la justice américaine lui donne raison
- ▶ 2016: Directive européenne dite « police-justice » encadre les traitements de mise en œuvre
- ▶ 25 05 2018: RGPD entre en application
- ▶ 13 03 2024: Législation sur l intelligence artificielle: IA act
- ▶ 24 04 2024: Projet de règlement pour un espace européen des données de santé.

# Le Rgpd est constitué de :

99 articles

173 considérants

**une règle d'or:**

*On ne collecte pour une finalité donnée qu'un minimum de données en assurant leur sécurité de la collecte à la destruction et pour un temps prédéfini.*

Pas de « au cas ou ».

# Les données à caractère personnel dites sensibles

art 4 du RGPD

## ► Les Données à caractère personnel :

Toute information se rapportant directement ou non à une personne physique identifiée ou identifiable tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

## ► Les données sensibles forment une catégorie particulière des données personnelles.

Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, **des données biométriques** aux fins d'identifier une personne physique de manière unique, des données **concernant la santé** ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

# Les finalités de la collecte de données dites sensibles exception art 9 RGPD

Les données de santé ou toutes données dites sensibles sont interdites à la collecte sauf pour les situations suivantes :

- a/ en cas de collecte du consentement explicite au traitement des données à caractère personnel pour une ou plusieurs finalités spécifiques (FORMATION PRIVEE)
- b/ aux fins de l'exécution des obligations en matière de droit du travail, de la sécurité sociale et de la protection sociale (VOLET RH)
- c/ pour la sauvegarde des intérêts vitaux de la personne concernée (URGENCES)
- f/ pour le droit en justice (MEDICOLEGALE)
- h/ pour les diagnostics médicaux, de la prise en charge sanitaire ou sociale (DOSSIER MEDICAL)

“

# La mise en conformité

*La CNIL peut effectuer un contrôle :*

*-sur site de 6h à 21h , dans le respect du secret médical.*

*-sur convocation*

”

**Le dossier RGPD comprend**

1/Le registre des traitements

2/La notice d information

3/ Le registre d incidents inclus dans beaucoup de logiciels métiers.

4/ L analyse d impacts sur la Protection des Données

5/ les clauses contractuelles des contrats des sous traitants

6/coordonnée du DPO désigné.

“

# Le registre des traitements

[Affichages réglementaires & RGPD - Ordre National des Chirugiens-Dentistes \(ordre-chirurgiens-dentistes.fr\)](http://ordre-chirurgiens-dentistes.fr)

”

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles.

# Définir le responsable du traitement

- ▶ Dans une SCM, les praticiens associés ont une patientèle distincte .
  - donc les dossiers médicaux (papier+ informatique) sont parfaitement séparés.
  - En cas de départ, l'associé a le droit d'emporter uniquement les dossiers correspondant à sa base patient.
- ▶ Dans une société d'exercice, c'est la société qui est titulaire de la patientèle.
  - En cas de départ, il est recommandé au praticien de conserver une copie des dossiers de ses patients ou de prévoir contractuellement un droit d'accès en cas de mise en jeu de sa responsabilité.
- ▶ Dans une collaboration libérale, en cas de départ, il faut distinguer :
  - les patients des titulaires dont le collaborateur doit garder une copie pour des raisons de responsabilité professionnelle.
  - Les patients des collaborateurs dont le collaborateur garde l'intégralité des dossiers.

# Les finalités

Avant toute collecte, il faut définir le cadre légal.

- ▶ 1/ le dossier médical
- ▶ 2/ les contrats de travail
- ▶ 3/ les sous traitants
- ▶ 4/ autres: recherche médicale, formations,..

1 collecte = un usage précis

# Évolution des usages sans détournement de finalité

- ▶ Il reste possible de définir un nouvel usage si l'une des deux conditions est réunie
  - ❑ consentement des personnes libre, spécifique, éclairée, univoque (registre des consentements à tenir)
  - ❑ le nouvel usage se fonde sur une disposition du droit de l'union ou droit de l'état membre.

## ▶ Art 5-1, alinéa b

La RGPD prévoit 3 finalités compatibles avec la finalité initiale:

- ❑ Archives publiques
- ❑ Recherche scientifique ou historique
- ❑ Statistiques

# Détournement de finalité

## ➤ Code pénal art 226-21

Le détournement de finalité est sanctionné de **300 000<sup>E</sup> d amendes et de 5 ans de prison**

## ➤ RGPD art 83-5

Le détournement fait l'objet d'une sanction administrative pouvant s'élever à 20 millions d'euros ou **4% du chiffre d'affaire mondial.**

## ➤ Article R4127-208

En vue de respecter le **secret professionnel**, tout chirurgien-dentiste doit veiller à la protection contre toute indiscretion des fiches cliniques, des documents et des supports informatiques qu'il peut détenir ou utiliser concernant des patients.

## ➤ Art226-13

La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un **an d'emprisonnement et de 15 000 euros d'amende.** »

# La tenue du dossier médical

- ▶ La notion de dossier médical peut être cernée en se reportant aux dispositions du 1er alinéa de l'article L. 1111-7 du Code de la santé publique qui traite du droit d'accès du patient audit dossier.
- ▶ l'ensemble des informations concernant la santé allant du diagnostique au suivi post opératoire :à savoir les résultats d'examen, les comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé, ...
- ▶ Minimisation de la collecte

# Durée de conservation du dossier médical

- 20 ans à compter de la dernière prise en charge du patient avec **attention**
  - ✓ une base active de 5 ans
  - ✓ puis archivage sur un support distinct avec accès restreint pendant 15 ans.
  - ✓ Suspension en cas de procédure.
- 40 ans pour les dispositifs médicaux incorporant une substance qui si elle est utilisée seule est susceptible d'être considérée comme un médicament dérivé du sang.
- 3 mois pour les FSE.

# Sécurité

une obligation qui pèse sur le responsable de traitement et le sous traitant

## ► Art RGPD 32-1

Le responsable du traitements doit assurer la sécurité des données de la collecte à la destruction.

- Mesures organisationnelles
- Hygiènes informatiques
- Mesures Physiques
- Mesures contractuelles sous traitants

# Exemple d'une de fuite de données

- ▶ En MARS 2021, un fichier contenant des informations personnelles et médicales concernant plus de 500 000 Français est diffusé sur le WEB.
- ▶ D'après les constatations de Libération, ces informations ont très vraisemblablement été prélevées dans des laboratoires qui utilisaient tous un même logiciel, Mega-Bus, de la société Dedalus France.
- ▶ Les nom, prénom, numéro de sécurité sociale, nom du médecin prescripteur, date de l'examen mais aussi et surtout des informations médicales (VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques) de ces personnes ont ainsi été diffusés sur internet.
- ▶ Sur la base des constatations effectuées lors des contrôles, la **formation restreinte** – organe de la CNIL chargé de prononcer les sanctions – a considéré que la société avait manqué à plusieurs obligations prévues par le RGPD, en particulier à l'obligation d'assurer la sécurité des données personnelles.
- ▶ Le 15 avril 2022, la **formation restreinte** de la CNIL a sanctionné la société DEDALUS BIOLOGIE d'une amende de 1,5 million d'euros, notamment pour des défauts de sécurité ayant conduit à la fuite de données médicales de près de 500 000 personnes.

# Mesures organisationnelles

- ❑ Politique de contrôle d'accès aux données : tracer et authentifier
  - ❑ Politique de mot de passe rigoureuse pour l'accès aux postes de travail et certains fichiers
  - ❑ Un mot de passe est unique, personnel , non recyclable et comporte entre 10 et 12 caractères.
  - ❑ utiliser un gestionnaire de mot de passe ( KEEPASS)
  - ❑ Séparer la Base active des archives
  
- ❑ Sensibiliser les utilisateurs :
  - ❑ Désigner un référent RGPD et un référent SSI
  - ❑ Messagerie professionnel et personnelle avec **protocole sécurisé** tels que HTTPS, IMAPS, POPS
  - ❑ documenter les procédures
  - ❑ les mettre à jour régulièrement.(audits RGPD tous les 3 ans)
  
- ❑ Politique de gestion des incidents ( registre incidents CNIL).
  - ❑ Mise à jour du registre des incidents pour RETEX
  - ❑ Malgré le registre doit être signalé à la CNIL toute violation de données personnelles susceptible de présenter un risque pour les droits et liberté des personnes dans un **délai de 72 heures**.
  - ❑ Si ces risques sont élevés, il convient d informer les personnes concernées.
  - ❑ En cas de cyberattaques, se rendre sur [Cybermalveillance.fr](https://www.cybermalveillance.fr)
  
- ❑ Prévoir la destruction du matériel informatique en fin de vie ou suivre les consignes de recyclages strictes de l ANSSI.



# KeePass

Keepass2 est un logiciel conseillé par ANSSI.  
Un seul mot de passe à retenir pour accéder à la base de donnée.  
Le logiciel liste les différents mots de passe et en génère en fonction des critères préétablis.

Database.kdbx - KeePass

File Group Entry Find View Tools Help

Shared.kdbx Database.kdbx

Title	User Name	Password	URL	Notes
Example 1	user@exa...	*****	https://exa...	Some notes.
Example 2	user@exa...	*****	https://exa...	Some notes.
Example 3	user@exa...	****		
Example 4	user@exa...	****		
Example 5	user@exa...	****		
Example 6	user@exa...	****		
Example 7	user@exa...	****		
Example 8	user@exa...	****		
Example 9	user@exa...	****		
Example 10	user@exa...	****		
Example 11	user@exa...	****		
Example 12	user@exa...	****		

Group: Internet Title: Example 2, User Name: user@example.net, Pa  
Creation Time: 16.07.2020 19:40:23, Last Modification Time: 16.07.2020 19:40:23

Some notes.

1 of 24 selected | Ready.

Add Entry

Create a new password entry.

Entry Advanced Properties Auto-Type History

Title:  Icon:

User name:

Password:

Repeat:

Quality:  108 Bits

URL:

Notes:

Expires: 6/ 6/2012 11:25:50 AM

Tools OK Cancel

## Messagerie sécurisée

24 04 2024: Projet de règlement pour un espace européen des données de santé.

### ► **Mon Sisra**

- ❑ Permet d'échanger des données de santé de patients, rapidement et en toute sécurité, avec les professionnels et structures intervenant dans la prise en charge.
- ❑ D'autres fonctions sont disponibles:
  - Réalisez des **demandes d'expertises** ou rendez des avis.
  - Réalisez des **téléconsultations par visioconférence**
  - **Accédez simplement à l'ensemble des services e-santé** de la région, en toute sécurité et sans codes d'accès à ressaisir

### ► **Mon espacesanté.fr**

- ❑ Mon espace santé est un espace numérique personnel et sécurisé, proposé par l'Assurance Maladie et le ministère de la Santé, qui a vocation à devenir le carnet de santé numérique interactif de tous les assurés.
- ❑ Messagerie pouvant être configuré à votre logiciel métier avec authentification cps.

## Hygiène informatique:

assurer la disponibilité, l'intégrité, la confidentialité des données collectées.

- ❑ Anticiper le risque de perte des données:
  - ❑ Sauvegarde: journalière, hebdomadaire
  - ❑ Chiffrement systématique des données sur les supports amovibles.
  - ❑ Utiliser des cloud certifiés HDS (Hébergeur de Données de Santé) et/ou **SecNumCloud**
- ❑ Anticiper le risque de divulgation des données:
  - ❑ Firewall via logiciel et/ou physique .
  - ❑ WIFI non partagé.
  - ❑ Navigation privée
- ❑ Mise à jour automatique des logiciels, antivirus sur le site de référence.
- ❑ Si plusieurs utilisateurs coexistent sur le serveur, faites installer
  - ❑ un compte administrateur (droit maximal pour installation des logiciels, mise à jour),
  - ❑ des comptes utilisateurs nominatifs (accès avec mot de passe)
  - ❑ et un compte invité ( droits limités)
- ❑ Séparer les usages pro et personnels
- ❑ Charte informatique

# La charte informatique

- Modèle sur site CNIL
- Pour respecter RGPD, c est une mesure forte voire indispensable.  
Cette charte fixe les règles d'utilisation des outils informatiques et précise les sanctions encourues
  
- ▶ Pour la mettre en place:
  - on informe le personnel ( CSE)
  - on fixe une date d entrée en vigueur
  - on annexe cette charte
    - ❖ Au contrat de travail ( avenant)
    - ❖ Au règlement intérieur (avis CSE art L2312-8 + exemplaire au greffe des Prudhommes R1321-2 code travail + exemplaire inspection travail)

## Exemple de **divulgaration par négligence**

- ▶ Utilisation d'un **mot de passe faible** ou recyclé.
- ▶ Inscription du mot de passe sur un **support accessible** à un tiers (post-it sous le clavier, tableau blanc, etc.) ;
- ▶ **Diffusion** à un tiers (collègue, ami, opérateur de service informatique, mot de passe envoyé par email, etc.) oralement ou par écrit (papier, mail, etc.) ;
- ▶ Authentification sur un service via un **protocole non sécurisé** tels que HTTP, IMAP, POP3, etc. au lieu de HTTPS, IMAPS, POPS ;
- ▶ Utilisation d'un ordinateur/smartphone qui ne soit pas de confiance et potentiellement **infecté** (cybercafé, ordinateur en libre accès dans un hôtel, etc.) ;
- ▶ Mot de passe enregistré sur le navigateur internet **sans protection.**

Mesures Physiques :  
prévenir risques en cas de cambriolage, incendie, accident, curiosité,...

- ❑ Principe du poste vide en fin de journée
- ❑ Mettre en veille lors de pause

*ctrl + ⌘ + Q sous Mac et touches Windows + L sous Windows).*

- ❑ Sécurités physiques
  - ❖ Alarme pour locaux,
  - ❖ Coffre fort pour carte CPS, disque dur externe,..
  - ❖ Pièce ou armoire à verrou pour archives papier
- ❑ Plan de continuité en cas de sinistre , accidents.
- ❑ Préserver la confidentialité : orientation des écrans, accompagnement des visiteurs,..
- ❑ Vérifier clauses des Assurances.

# 07 février 2024

- ▶ 22 01 2024 : Microsoft est visé par une cyberattaque .
- ▶ 07 02 2024 : fuite de données pour les opérateurs Viamedis et Almerys
- ▶ L'attaque s'est faite par l'usurpation d'identifiants et mots de passe de professionnels de santé.
- ▶ Au total, cette fuite de données concerne **plus de 33 millions de personnes**. Les données concernées sont, pour les assurés et leur famille, **l'état civil, la date de naissance et le numéro de sécurité sociale, le nom de l'assureur santé ainsi que les garanties du contrat souscrit**.
- ▶ Devant l'ampleur de la violation, une enquête de la CNIL est en cours pour déterminer si les mesures de sécurité ont été appropriées.

# Les clauses contractuelles des sous traitants

Avant de signer un contrat de sous traitante:

1/ la base légale: intérêt légitime?

2/le contrat doit préciser conformément art 28 du RGPD

- Le type de données à caractère personnel collectées avec principe de minimisation
- La durée de conservation des données et le mode de destruction.
- Les obligations (sécurité, gestion des incidents,..)
- Les droits du sous-traitant.
- SI transferts de données hors UE:
  - le pays est il conforme (suisse, depuis 07 2023 , certains organismes EU) ou à risques ( Russie, Corée)?
  - Si à risques, clauses contractuelles types contraignantes.

# AIPD :

## Analyse d Impact relative à la protection des données

- ▶ Décrire un traitement de manière détaillée avec cartographie des risques
- ▶ Évaluer sa conformité à la RGPD
- ▶ Identifier les risques que ce traitement peut engendrer sur les droits et libertés
- ▶ Obligatoire si 2 des 9 critères suivants est rempli= AIPD
  - Évaluation (y compris profilage)
  - Décision automatique avec effet légal ou similaire
  - Surveillance systématique
  - Collecte de données sensibles
  - Collecte de données personnelles à grande échelle
  - Croisement de données
  - Personnes vulnérables
  - Usage innovant
  - Exclusion du bénéfice d'une loi ou d'un contrat
- ✓ Logiciel gratuit CNIL PIA ou audit externe

# Le DPO :Officer Data Protector

le DPO a une Mission d informations , de conseil, de contrôle et d intermédiaire

À désigner , si plus **de 10 000 dossiers** (cabinet de groupe).

le DPO peut être :

- ❑ interne à la structure ( Mooc cnil + Mooc anssi)
- ❑ externe , un réfèrent au sein de la structure sera tout de même requis
- ❑ mutualisé

# INTELLIGENCE ARTIFICIELLE

- ❑ 13 03 2024: Législation sur l'intelligence artificielle rentre en application (IA act).

Elle retient le principe de transparence et de garantie humaine .

Ce règlement se base sur une échelle de risques et prévoit des obligations proportionnées aux risques.

Le règlement prévoit des sanctions allant jusqu'à 7% du CA mondial.

- ❑ Projet Oralien est un programme de l'UFSBD qui propose une solution de télémédecine en EHPAD. UFSBD et Dental monitoring ont missionné ETHIK IA pour assurer la garantie humaine de leur algorithme.
- ❑ Chat gpt est un chatbot proposé par OPEN IA dont la transparence est discutée

MARS 2023 OpenAI, propriétaire de ChatGPT, accusée par l'Italie d'enfreindre les règles européennes relatives à la protection des données.

SEPT 2023: Un chercheur polonais en cybersécurité a porté plainte contre OpenAI pour violation du RGPD.

29 04 2024 :une association autrichienne a annoncé déposer plainte contre ChatGPT pour usage abusif des données personnelles et usurpation des droits d'auteur.

# Cas particuliers des mineurs

## RGPD- considérant 38

Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leur droits liés au traitement des données à caractère personnel.

### Exemple pratique: Denta poche

- ▶ Application ODF sur smartphones:
  - ❖ les rendez vous
  - ❖ la messagerie entre parents/ adolescents et cabinet orthodontique
  - ❖ partages de document
  - ❖ Fonction accueil
- ▶ Démarche de sécurisation:
  - ❖ Principe de minimisation des données
  - ❖ Consentement éclairé mineur/ parent



# Cas particulier de la recherche Médicale.

- La recherche médicale a vocation interne ( taux de réussite endo) ne demande pas de démarches particulières.
  
- En cas de recherches externes au cabinet, raisonnement en 2 temps
  - ❖ la **création de l'entrepôt de données** en tant que tel (c'est-à-dire la collecte et la conservation des données dans une base unique pendant une plus longue durée) ;
  
  - ❖ les **projets de recherches, d'études ou d'évaluations réalisés à partir des données conservées dans l'entrepôt** par le même responsable de traitement ou d'autres organismes.
  
  - ❖ Formalités auprès de la CNIL et du Health Data Hub
  
- Avant de donner une donnée issue d un dossier médical,
  - ❖ Demander la méthodologie de référence (MR004-MR 003-MR 002-MR001) et la notion de consentement.
  
  - ❖ Informer le patient
  
  - ❖ Enregistrer cette finalité dans votre registre des traitements.

# Droits des personnes

La RGPD donne aux personnes concernées par un traitement plusieurs droits:

1. L information
2. L accès
3. *Rectification des données*
4. L opposition
5. *Effacement*
6. Limitation du traitement
7. Portabilité: transfert de données/dossiers médicaux.
8. Prise de décision individuelle automatisée : possibilité de refuser un profilage

N est pas un droit absolu: c'est pourquoi nous devons encadrer la collecte des données et justifier de sa finalité.

# La notice d'information

- La RGPD pose un principe de loyauté et de transparence vis à vis des personnes concernées sur la nature de la collecte et des finalités.
- **RGPD art 12-1**
  - Les informations doivent être communiquées d'une façon concise, transparente, compréhensible et aisément accessible, en termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant.
- **Site CNOCD: fiche F4 à afficher en salle d attente**

# Droit d'accès

Art 1111-7 du code de santé publique prévoit l'accès direct du patient ou par l'intermédiaire d'un médecin .

La modalité d'accès est la suivante:

- ❖ Demande d'accès au dossier médical (annotations comprises )adressé au praticien avec enregistrement de la date de réception.
- ❖ Vérification de l'identité du demandeur.
- ❖ Réponse à partir de la date de réception
  - ❑ Sous 8 jours si le dossier date de moins de 5 ans ( base active)
  - ❑ Sous 2 mois si les données médicales datent de plus de 5 ans donc archivées.
  - ❑ La consultation sur place ou l'envoi par mail sont gratuits. En revanche, l'administration peut exiger le paiement des frais exposés pour la reproduction et les frais d'envoi de documents administratifs.
- ❖ Plus d'informations: [Les modalités de communication | La CADA](#)  
<https://www.cada.fr/particulier/les-modalites-de-communication>

# VIDEO SURVEILLANCE et cabinets médicaux

## ➤ Cas particulier des cabinets médicaux:

Votre cabinet médical est considéré comme un lieu ouvert au public, au sens du code de la sécurité intérieure.

Pour installer un système de vidéosurveillance, vous devez obtenir une **autorisation de la préfecture** valable cinq ans. La demande d'autorisation peut être effectuée en ligne sur le site du ministère de l'Intérieur.

Ensuite, vous **devez déclarer votre système de vidéoprotection** en complétant le formulaire CERFA n° 13806\*03.

**Informez vos patients** de façon claire et permanente de l'existence d'un système de vidéoprotection, par exemple en affichant un pictogramme caméra dans votre cabinet ou votre salle d'attente.

- Acquisition d'image pour levée de doutes : insister sur **le contrat de sous traitant**
- **Durée de conservation entre 7 jours et 1 mois**
- vigilance sur la position de la caméra ( salle de soins, salle de repos)
- Les référents sureté de la gendarmerie peuvent vous aider: [Accueil \(referentsurete.fr\)](http://Accueil.referentsurete.fr)

# ENTREPRISE SOUS SURVEILLANCE VIDÉO

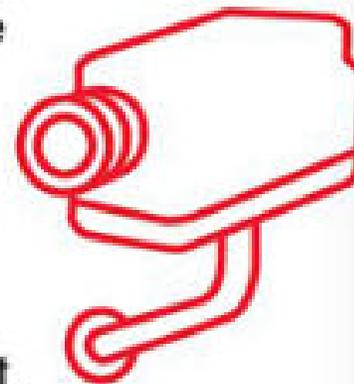
Etablissement placé sous vidéosurveillance par ABCD pour la sécurité des personnes et des biens.

Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité de la société ABCD et par les forces de l'ordre.

Pour exercer vos droits Informatique et Libertés, notamment votre droit d'accès aux images qui vous concernent, ou pour toute information sur ce dispositif, vous pouvez contacter notre délégué à la protection des données en écrivant à [dpo@abcd.fr](mailto:dpo@abcd.fr) ou à l'adresse postale suivante : XXXX.

Pour en savoir plus sur la gestion de vos données personnelles et vos droits, rendez-vous sur l'intranet ABCD / le règlement intérieur – Rubrique « Politique de protection des données »

Vous pouvez introduire une réclamation auprès de la CNIL sur [cnil.fr/plaintes](http://cnil.fr/plaintes)



# Télésecrétariat et écoute téléphonique

## ► **L'information des personnes concernées**

A l'instar de tout autre traitement, le responsable de traitement a l'obligation de délivrer à la personne concernée par l'enregistrement l'ensemble des informations prévues au titre de l'article 13 du RGPD.

Une **mention orale** en début de conversation faisant état de l'existence du dispositif d'enregistrement, de la finalité poursuivie et de la possibilité éventuelle de conclure le contrat par d'autres moyens.

## ► **Le droit d'accéder à l'enregistrement téléphonique**

A toutes fins utiles, la Commission rappelle également qu'en vertu du droit d'accès (art. 15 du RGPD) la personne concernée peut à tout moment solliciter communication de l'enregistrement.

# Merci de votre Attention