AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES (APDP)

ATELIER DE FORMATION À L'INTENTION DES ACTEURS DU SECTEUR DE LA SANTÉ

Thème : Les obligations du Responsable de Traitement en matière de données de Santé

Intervenant : Emmanuel ZOSSOU

Consultant informatique et
Protection des données personnel et
de la vie privée

COTONOU LE 4 OCTOBRE 2022

Sommaire

INTRODUCTION

- **Avec le développement d’internet, d’énormes quantités de données personnelles circulent sur tous les réseaux.**

- **La gestion des données est devenue un enjeu majeur du XXIème siècle.**

- **Les outils informatiques nous accompagnent tous les jours dans tous les domaines, et les multiples cyber-attaques qui composent l'actualité ne cessent de nous rappeler que les données sont convoitées par de nombreuses personnes.**

- **Ce phénomène a pris de l’ampleur au fil des années, à tel point qu’il fallait le contrôler et le réguler sans contraintes majeures pour les responsables de traitement.**

INTRODUCTION

- **Afin :**

  - de protéger les citoyens contre les traitements illégaux et la collecte sauvage des informations qui les concernent et

  - de renforcer le niveau de protection de la vie privée et des libertés des personnes au Bénin,

  la loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin a été modifiée donnant lieu à la loi n°2017-20 du 20 avril 2018 portant Code du numérique (CDN) en République du Bénin qui consacre son livre V à la protection des données personnelles.

- **Ce code, en vigueur depuis 2018, concerne également les professionnels de santé.**

INTRODUCTION

- **Cette nouvelle loi vise, à:**

  - Simplifier les formalités de :

  - ✓ **demandes d'avis,**
  - ✓ **de déclaration et**
  - ✓ **d'autorisation auprès de l'autorité de protection des données;**

  - responsabiliser davantage les responsables de traitement, puis à

  - créer une nouvelle fonction, selon le cas, au sein de l'entreprise, désignée sous le nom de «Délégué à la Protection des Données personnelles (DPD ou DPO) ».

A-Contexte dans le secteur de la Santé

1. **Multiplication et banalisation des données de santé**

2. La **Multiplication des attaques**

   a) Les fuites de données

   b) Les piratages, destructions et rançonnages de données

A-Contexte dans le secteur de la Santé

1) Multiplication et banalisation des données de santé

- L’informatisation des hôpitaux, des cabinets médicaux et paramédicaux, des pharmacies et des laboratoires, est une réalité depuis plusieurs années.
- Tant que les données restaient stockées localement, sans connexion à internet, le risque de fuite de données, qu’elle soit accidentelle ou intentionnelle, était faible.
- Mais avec le recours croissant aux échanges en ligne entre acteurs de santé, à la télémédecine et au stockage dans le *cloud*, les données de santé sont appelées à circuler mondialement et à être hébergées chez de nombreux prestataires.
- Les risques sont multipliés dans les mêmes proportions.

A-Contexte dans le secteur de la Santé

1) Multiplication et banalisation des données de santé

- Au-delà de ces échanges entre professionnels, se développe également la pratique consistant à mesurer en continu son activité physique, appelée automesure connectée, ou quantified Self - (nombre de pas…), voire ses paramètres (tension, rythme cardiaque, mais aussi glycémie…), en vue d'adopter un mode de vie sain ou de surveiller un marqueur particulier.

- Nombre de pas, poids, heures de lever et de coucher..., dans une première approche, on pourrait être tenté de considérer comme anodines ces données prises isolément et en dehors de tout contexte.

- On ne peut semble-t-il considérer que les données collectées dans le cadre des outils et applications du *quantified self (QS)* sont toutes, par nature, des données de santé.

A-Contexte dans le secteur de la Santé

1) Multiplication et banalisation des données de santé

- Cependant, certaines informations, prises indépendamment et en valeur absolue, peuvent dans des situations précises être considérées comme données de santé, en raison de l'information objective qu'elles sont susceptibles de transmettre.
- Par exemple, un poids objectivement excessif peut révéler une pathologie telle que l'obésité.
- Or ces données sont souvent transférées à l’entreprise qui commercialise le capteur, et qui fournit des applications d’analyse des résultats sur mobile ou sur ordinateur. Elles sont parfois également publiées sur un réseau social, dans un objectif d’émulation (ex : perte de poids).
- Ces données intéressent de nombreux acteurs, et au premier rang desquels les assureurs et mutuelles de santé.

A-Contexte dans le secteur de la Santé

1) Multiplication et banalisation des données de santé

- Des assureurs américains proposent déjà des tarifs préférentiels pour les clients acceptant de porter des objets connectés afin de prouver leur activité physique.

- Au-delà du problème de la marchandisation des données à des tiers (compagnies d'assurances, par exemple), une autre problématique quant à la protection des données peut être soulevée.
- En effet, le QS étant une offre numérique, la question de la sécurité de la sécurité des données peut se poser, notamment pour les utilisateurs qui enregistrent des données personnelles et/ou de santé dans les applications de quantification de soi.

- **Faut-il réguler cette activité ?**

A-Contexte dans le secteur de la Santé

2) Multiplication des attaques

- Le corollaire de la multiplication des échanges de données de santé, est la fuite accidentelle ou les attaques

a) Les fuites de données

Des données de santé peuvent se retrouver en ligne suite à une négligence ou à un accident.

Cette fuite de données ne résulte pas d'une malveillance, mais d'une insuffisance de mise en œuvre des règles de sécurité.

Des dossiers peuvent ainsi se retrouver référencés par un moteur de recherche comme Google et consultables par tout un chacun.

A-Contexte dans le secteur de la Santé

2) Multiplication des attaques

b) Les piratages, destructions et rançonnages de données

Les données de santé peuvent également faire l'objet d'attaques délibérées.

La motivation peut être le vol d'informations.
L'attaque peut également avoir pour but de les rendre inutilisables, que ce soit pour entraver le fonctionnement des soins ou pour rançonner la victime.

Aux États-Unis, plus de 200 millions de dossiers médicaux auraient ainsi été dérobés par piratage des systèmes.

Les attaques de « rancongiciels » deviennent courantes : l'attaquant bloque les données en les chiffrant, et réclame une rançon pour permettre le déchiffrement. En 2016, l'hôpital Hollywood Presbyterian Medical Center de Los Angeles avait dû payer 17.000 dollars pour récupérer ses données.

A-Contexte dans le secteur de la Santé

2) Multiplication des attaques

b) Les piratages, destructions et rançonnages de données

Ces attaques se sont multipliées en 2017 avec le virus Wannacry, qui a touché des dizaines d'hôpitaux, notamment au Royaume-Uni. « L'attaque a sérieusement désorganisé des dizaines d'hôpitaux, contraints d'annuler certains actes médicaux et de renvoyer des ambulances vers d'autres établissements ».

On ne peut donc que rappeler l'importance d'une application stricte des règles de sécurité des systèmes d'information, pour éviter ce type de situation et limiter les dégâts en cas d'attaque : mise à jour permanente des applications et des systèmes d'exploitation, limitation des droits utilisateurs, gestion des mots de passe d'administrateur, systématisation des pare-feux et des antivirus, sauvegardes régulières des données sur un serveur distinct…

B- Quelques Définitions et Rappels :

a) Le RT
b) Le sous-traitant
c) Les principaux types de RT
d) Les données sensibles
e) Données de santé
f) Base légale du traitement des données de santé

1- Les obligations du Responsable des traitement : Définitions

a) Le Responsable de traitement

- **Le CDN définit le Responsable de traitement comme**
  - **toute personne physique ou morale, toute autorité publique, tout service ou tout autre organisme ou association** *(cette 1ère partie de la definition désigne qui peut être responsable du traitement)*
  - **qui, seul ou conjointement avec d'autres** (cette 2è partie rappelle que la responsabilité d'un traitement de données peut reposer sur une ou plusieurs personnes d'où l'idée de co-responsabilité),
  - **prend la décision de collecter et de traiter de données à caractère personnel et en détermine les finalités et les moyens (article 1).** *(cette 3è partie de la définition précise qui prend les décisions importantes concernant le traitement.)*
- **En tant que tel, le responsable de traitement est, avec ses éventuels sous-traitants et l'Autorité, le principal agent de protection des données à caractère personnel.**
- **Le CDN traite le RT à sa juste valeur en mettant à sa charge de nombreuses d'obligations qui le responsabilise.**

1- Les obligations du Responsable des traitement : Définitions

b) Le Sous-traitant

- Le responsable du traitement peut décider de déléguer tout ou partie des activités de traitement à une organisation extérieure.
- Le sous-traitant est une personne physique ou morale, qui traite les données à caractère personnel, **sans possibilité de faire quelque traitement que ce soit sans l'autorisation expresse** du responsable de traitement.

- Le sous-traitant a pour mission donc d'exécuter des tâches sur les instructions et **sous la responsabilité** du responsable du traitement.

NB

- En cas de recours à un sous-traitant, le responsable du traitement doit choisir un sous-traitant qui apporte **des garanties suffisantes** au regard des **mesures de sécurité technique** et **d'organisation** relatives aux traitements à effectuer.
-

Définitions et rappels

- **Responsables de traitements dans le secteur de la Santé**

On peut considérer comme responsables de traitement dans le secteur de la santé les:

- ❑ Professionnels de santé libéraux
- ❑ Cabinets médicaux et paramédicaux
- ❑ Établissements de santé
- ❑ Fabricants de dispositifs médicaux
- ❑ Pharmacies d’officine
- ❑ Laboratoires d’analyse médicale
- ❑ Services de santé au travail
- ❑ Etc.

Définitions et rappels

- **Données sensibles :** (art 01)
- Le CDN définit comme données sensibles, « Toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, à la génétique, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ; »

- Il est **interdit** de recueillir et de traiter ces **données (**Article 394)

- **Donnée de santé** (art 01) **:**
- Le CDN définit comme données concernant la santé : « toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestatio de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personn ; »

Définitions et rappels

- **On distingue 3 catégories de données de santé :**
- celles qui sont des données de santé **par nature** : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- celles, qui du fait de leur croisement avec d'autres données, deviennent des données de santé e ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'un personne : **croisement** d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques…), croisement de la tension avec la mesure de l'effort, etc.
- celles qui deviennent des données de santé en raison de leur **destination**, c'est-à-dire de l'utilisation qui en est faite au plan médical.
- Les deux dernières catégories peuvent regrouper un grand nombre de données. Ceci permet un protection plus élevée des personnes et invite dans une certaine mesure le responsable de traitement à porter une attention particulière à toute donnée pouvant révéler de loin ou de près une information sur la santé d'une personne.
-

Définitions et rappels

- **Base légale du traitement des données de santé**
- Du fait de la sensibilité des données de santé, leur traitement informatisé est particulièrement encadré par le droit.

- En effet, les données de santé constituent des données à caractère personnel, et même des données dites « sensibles ».

- Elles relèvent donc à ce titre des dispositions concernant les données personnelles, au niveau du Code du numérique (art. 394).

- Toutefois on pourrait ajouter des dispositions spécifiques, justifiées par le caractère médical des données de santé, qui impose des contraintes particulières de fiabilité, de disponibilité et de sécurité, afin de garantir notamment la continuité des soins.

Définitions et rappels

- **Le principe en matière de traitement de données de santé est :**

- Interdiction de traiter des données relatives à la santé ;

- Pour traiter des données de santé, il faut justifier de l'une des exceptions de l'alinéa 2 de l'article 394 du CDN

Définitions et rappels

- **Ces exceptions à ce principe d'interdiction** sont :

♣ Le consentement explicite

♣ Obligations liées au droit du travail, protection sociale, sécurité sociale

♣ Sauvegarde des intérêts vitaux de la personne

♣ Les traitements mis en œuvre par une association ou autre organisme à but non lucratif si :

- le traitement se rapporte exclusivement aux membres de l'organisme ou personnes entretenant des contacts réguliers et
- la personne concernée a donné son consentement pour les données transmises hors de l'organisme

Définitions et rappels

- **Ces exceptions à ce principe d'interdiction** :

♣ Données rendues publiques par la personne concernée

♣ Constatation, exercice ou défense d'un droit en justice

♣ Motifs d'intérêt public important

♣ Médecine préventive, diagnostics médicaux, prise en charge sanitaire ou sociale ou gestion des systèmes et services de soins en santé

♣ Motifs d'intérêt public dans le domaine de la santé publique

♣ Recherche scientifique, fins archivistiques ou statistiques

♣ etc.

A. Les obligations des Responsables de traitement

a) Les obligations de redevabilité
b) Les obligations à l’égard des personnes
c) Les obligations à l’égard de l’Autorité
d) Les obligations de diligence préalable
e) Les obligations en cas de transfert de données

2- Les obligations du Responsable de traitement

A- l'obligation de redevabilité (l'accountability)

- À partir de l'avènement du CDN, le responsable du traitement doit être « accountable » ou pour le dire en français, le responsable du traitement doit être « en mesure de rendre des comptes »

- Ce nouveau principe d'«accountability» vise à davantage responsabiliser les responsables de traitement en leur laissant plus de marge de manœuvre dans les choix qu'ils font afin d'assurer la conformité de leur traitement avec le CDN. Dans cette optique, on passe d'un modèle de contrôle à priori (lourd et peu efficace) à un modèle de contrôle a posteriori.

- Ce basculement entraine **trois conséquences :**
  – suppression d'un certain nombre de formalités préalables au traitement ;
  – responsabilisation des responsables de traitement ;
  – renforcement des pouvoirs de contrôle et de sanction.

Le responsable du traitement a donc plus de liberté qu'auparavant concernant les mesures à mettre en place pour assurer le respect du cadre légal, mais il est responsable de ses choix et doit pouvoir démontrer qu'il a bien fait le nécessaire.

2- Les obligations du Responsable de traitement

A- l'obligation de redevabilité (l'accountability) - suite

Cette plus grande flexibilité permet également à chaque responsable du traitement de développer les procédures les plus adaptées aux spécificités du traitement qu'il effectue.

Le responsable du traitement est certes plus responsabilisé, mais le CDN ne le laisse pas complètement libre sur la manière de se conformer au règlement et impose certaines mesures qui sont particulièrement importantes et nécessaires.

Nous pensons notamment à l'obligation pour le responsable:

- de tenir un registre,
- d'effectuer des analyses d'impact,
- de désigner un DPD,
- de respecter les principes de « privacy by design » et « privacy by default »,
- …etc.

Il peut être noté que bon nombre de mécanismes présents dans le CDN d' écoulent d'une manière ou d'une autre de ce principe de recevabilité.

2- Les obligations du Responsable de traitement

A- l'obligation de redevabilité (l'accountability) - suite

Afin de se conformer au principe d'accountability, l'organisme doit tenir une documentation en interne qui décrit les traitements ainsi que les mesures prises pour assurer la conformité de ces traitements.

Parmi ces documents, il faut surtout porter une attention particulière à la conservation des autorisations conférées par l'APDP pour tel ou tel traitement.

En effet, dans le domaine de la santé, l'APDP doit être sollicitée dans certains cas notamment pour les traitements de recherche et le traitement ne peut être mis en œuvre qu'après avoir reçu son autorisation.

2- Les obligations du Responsable de traitement

B- Les obligations à l’égard des personnes: obligations d’information

1- les mentions d’information.

2- Les obligations de notification

3- L'obligation de réponse aux demandes d’exercice de droit

4- Le consentement

2- Les obligations du Responsable de traitement

B- l'obligation à l'égard des personnes concernées: obligations d'information

1- LES MENTIONS D'INFORMATIONS

Les articles 415 et 416 du CDN énumèrent les informations à communiquer en cas de collecte directe auprès de la personne concernée et en cas de collecte indirecte.

- Le responsable du traitement ou son représentant doit fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, au moins les informations suivantes :

1. son identité et l'adresse de sa résidence habituelle;
2. le cas échéant, les coordonnées du délégué à la protection des données ;
3. la ou les finalités déterminées du traitement auquel les données sont destinées;
4. la durée de conservation des données ;
5. le ou les destinataires auxquels les données sont susceptibles d'être communiquées ;
6. le fait de pouvoir demander à ne plus figurer sur le fichier ;

2- Les obligations du Responsable de traitement

B- l’obligation à l’égard des personnes OU obligation d’information

1- LES MENTIONS D’INFORMATIONS (suite)

7. l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de prospection notamment commerciale, caritative ou politique

8. le caractère obligatoire ou non de la réponse, le caractère réglementaire ou contractuel ainsi que les conséquences éventuelles d'un défaut de réponse ;

9. l’existence d’un droit d’accès aux données la concernant et de rectification ou l’effacement de ces données ;

10. lorsque le traitement est fondé sur l’existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

11. le droit d’introduire une réclamation auprès de l'Autorité ;

12. l’éventualité de tout transfert de données à destination d’États tiers.

2- Les obligations du Responsable de traitement

B Les obligations à l'égard des personnes: obligation d'information

2- LES OBLIGATIONS DE NOTIFICATION

En cas de violation de données subie, le RT est tenu de notifier l'incident aux personnes concernées.

La notification doit se faire sans délai à chacune des personnes concernées.

3- L'OBLIGATION DE RÉPONSE AUX DEMANDES D'EXERCICE DE DROIT

Le RT est tenu de répondre à une demande d'exercice de droit. (Droit d'accès, de rectification, d'opposition, droit de portabilité,….)

2- Les obligations du Responsable de traitement

B Les obligations à l'égard des personnes: LE CONSENTEMENT

-Le recueil du consentement

- Les données de santé peuvent être traitées dans le cas où le consentement de la personne a été collecté au préalable.
- Toutefois, cette exception introduite à l'article «394 du CDN ne peut être considérée comme valide que lorsque les principes généraux du consentement ont été respectés.
- En effet, le consentement doit être collecté de manière:
    - **libre**,
    - **spécifique**,
    - **éclairé** et
    - **univoque**.
- La personne concernée ne doit notamment pas être forcée à donner son accord et il ne doit pas y avoir un doute quant à la volonté de consentir.

2- Les obligations du Responsable de traitement

B Les obligations à l'égard des personnes: LE CONSENTEMENT

- **Les autres exceptions**

  En plus de l'exception portant sur la collecte du consentement, d'autres exceptions existent permettant d'autoriser le traitement des données de santé, notamment dans les cas suivants :

  - Respect des obligations légales.
  - Sauvegarde des intérêts vitaux.
  - Données ont été rendues publiques par la personne concernée.
  - Pour des motifs d'intérêt public.
  - Nécessaire aux fins de la médecine préventive ou la médecine du travail.
  - A des fins archivistiques, de recherche ou statistiques.

2- Les obligations du Responsable de traitement

C- LES OBLIGATIONS A L'EGARD DE L'AUTORITE

1- Les obligations de sécurité des données de santé

2- L' obligation de tenue de registre de traitement

3- Les obligations de notification des violations

2- Les obligations du Responsable de traitement

C- LES OBLIGATIONS A L'EGARD DE L'AUTORITE

2- L'OBLIGATION DE SÉCURITÉ DES DCP [ART. 426]

Le responsable du traitement a obligation de mettre en œuvre des mesures de sécurité afin d'assurer que les données ne sont pas détruites, modifiées ou divulguées indûment, que ce soit par accident ou suite à une action malveillante.

Ces mesures doivent être aussi bien

- **techniques** (*installation d'antivirus sur les serveurs, mise à jour permanente des logiciels et des systèmes d'exploitation, chiffrement des échanges, journalisation des accès, attribution de codes d'accès personnels*…)
- **qu'organisationnelles** (*limitation des personnes ayant accès aux données, limitation des durées de conservation, sauvegarde régulière des données, redondance des serveurs et des alimentations…).*

2- Les obligations du Responsable de traitement

C- LES OBLIGATIONS A L'EGARD DE L'AUTORITE

2- L'OBLIGATION DE SÉCURITÉ DES DCP [ART. 426]

En cas de violation de sécurité *(perte ou fuite de données),* la loi impose une notification immédiate à l'APDP par le responsable du traitement.

La notification décrit la nature de la violation, les données concernées, les conséquences probables et les mesures de ré-médiation adoptées ou envisagées.

Si cette violation entraîne un risque élevé pour les personnes concernées, le responsable du traitement doit également avertir ces personnes.

2- Les obligations du Responsable de traitement

C- LES OBLIGATIONS A L'EGARD DE L'AUTORITE

1- L'OBLIGATION DE TENUE DU REGISTRE DE TRAITEMENT

Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité.
Le responsable du traitement, et le cas échéant, son représentant met le registre à la disposition de l'Autorité sur demande.

En outre, conformément à l'article 387 dernier alinéa, le RT est tenu de présenter un rapport annuel de traitement pour démontrer à l'Autorité que son activité de traitement est conforme aux prescriptions du CDN.

2- Les obligations du Responsable de traitement

C- LES OBLIGATIONS A L'EGARD DE L'AUTORITE

3- L'OBLIGATION DE NOTIFICATION DES VIOLATIONS

Le CDN oblige le responsable du traitement à notifier, sans délai, à l'Autorité et à la personne concernée toute rupture de la sécurité ayant affecté les données à caractère personnel de la personne concernée (CDN, art 427 al 1er).

La notification du responsable du traitement doit contenir les mêmes informations que dans le cas d'une communication à la personne concernée.

Pour éclairer les usagers, l'Autorité a mis en ligne sur son site www.apdp.bj un formulaire de signalement qui spécifie plus clairement les informations à transmettre.

2- Les obligations du Responsable de traitement

D- LES OBLIGATIONS DE DILIGENCES PREALABLES

1- REGIME DE DÉCLARATION PRÉALABLE

Aux termes de l'article **405** du CDN, une déclaration préalable est requise pour « les traitements automatisés ou non automatisés exécutés par des organismes publics ou privés et comportant des données à caractère personnel ».

2- REGIME D'AUTORISATIONS

Selon l'article **407** CDN une demande d'autorisation doit être présentée par le responsable traitement ou son représentant à l'APDP préalablement au traitement dans les cas ;

- ✓ Actes d'état civil (naissance, mariage, décès, carte d'identité, passeport ,……) ;
- ✓ Données biométriques ;
- ✓ Interconnexion de fichiers ;
- ✓ Transferts de données hors CEDEAO ;
- ✓ Traitements automatisés relatifs aux difficultés sociales des personnes;
- ✓ Autres Traitements déterminés par l'APDP ;
- ✓ ……etc.

2- Les obligations du Responsable de traitement

D- LES OBLIGATIONS DE DILIGENCES PREALABLES

3- REGIME D'AVIS

- Selon l'article 411 du CDN, « … Les traitements des données à caractère personnel opérés pour le compte de l'État, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont autorisés par décret pris en Conseil des ministres après avis motivé de l'Autorité.
- Ces traitements portent sur :
  - ✓ La sûreté de l'État, la défense ou la sécurité publique ;
  - ✓ La prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
  - ✓ Le recensement de la population ;
  - ✓ Les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;
  - ✓ ….etc.

2- Les obligations du Responsable de traitement

D- LES OBLIGATIONS DE DILIGENCES PREALABLES

4- EXCEPTIONS ET DISPENSES

- Dans le souci d'alléger aux RT l'obligation de déclaration notamment, le CDN renonce à la déclaration préalable :

  a) En présence de données courantes, sous réserve du respect des normes de l'APDP ;

  b) En l'absence de risques d'atteinte aux droits et libertés individuelles sauf si le traitement est mis en œuvre par une autorité publique et

  c) Après désignation d'un DPO tenant à jour le registre de traitement et maintenant le contact avec l'Autorité.

Par ailleurs, le CDN accorde une dispense de formalités à tout traitement mis en œuvre :

- Pour un usage personnel et domestique ; - Pour la tenue d'un registre privé ;
- Pour la tenue de comptabilité générale ; - Pour la gestion de la paie ;
- Pour la gestion des fournisseurs et
- Pour les applications développées par les associations loi 1901 ne concernant que leurs membres (non destinées au public.)

2- Les obligations du Responsable de traitement

E- LES OBLIGATIONS EN CAS DE TRANSFERT DE DONNEES

Un transfert, à un pays tiers, ou à une organisation internationale de données à caractères personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si les conditions définies dans le livre V sont respectées par le responsable du traitement et le sous-traitant (code du numérique, art 391).

- **1- TRANSFERTS FONDÉS SUR UNE DÉCISION D'ADÉQUATION**

Il s'agit d'une liste préétablie de pays assurant un niveau de protection adéquate des données à caractère personnel, à la suite d'un examen approfondi des dispositions légales mises en place par ces pays et de la pratique.

Exemple **de niveau d'adéquation des pays dans le monde**

- **2- TRANSFERT MOYENNANT DES GARANTIES APPROPRIÉES**
  - **Transfert décrété par le conseil des ministres après avis de l'APDP en présence de garanties appropriées ou**
  - **Transfert autorisé par l'APDP en présence de garanties appropriées**

CONCLUSION

- Tout organisme traitant des données de santé est soumis à un certain nombre d'obligations portant sur les modalités de mise en œuvre des traitements des données à caractère personnel.

- Les principes généraux du CDN doivent être respectés et des mesures particulièrement renforcées doivent être mises en place au vu du caractère sensible de ces données.

Merci pour votre aimable attention

Pour plus de renseignements rendez-vous sur le site de l'APDP aux liens suivants :

- https://www.apdp.bj
- https://apdp.bj/les-outils-de-la-conformite/
- https://apdp.bj/procedures/