AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'informatique doit respecter l'identité humaine, les droits de l'homme, la vie privée et les libertés

FORMATION DES DELEGUES A LA PROTECTION DES DONNEES PERSONNELLES

THEME : DPDP : Rôle et mise en place

PRESENTE PAR : Emmanuel ZOSSOU

Ancien Commissaire à la CNIL-BENIN

Cotonou le 19 Décembre 2022

FORMATION DES DELEGUES A LA PROTECTION DES DONNEES PERSONNELLES

Le métier de DPDP se hisse à **la première place des métiers les plus recherchés sur LinkedIn en France**.

Sommaire

Introduction

- Entre expertise informatique, juridique, qualité et conformité, le Délégué à la Protection des Données Personnelles (DPDP) accompagne et conseille les organismes afin d'assurer leur conformité en matière de traitement de données personnelles.
- Exerçant ses missions dans tous les types d'organisme (entreprises, associations, administrations ou collectivités locale), il a également pour rôle d'assurer le contact avec l'Autorité de Protection des Données Personnelles (APDP) et les différentes personnes concernées (salariés, usagers, patients, fournisseurs, etc.).

A. DPDP :
champs d'application et notions

1. Contexte et facteurs d'évolution du métier
2. Genèse de la protection des données au Bénin
3. Définitions /rappels
   a) Données personnelles
   b) Données sensibles
   c) Traitement de données personnelles
   d) Responsable de Traitement
   e) Délégué à la protection des données Personnelles (DPDP)

1- Contexte et facteurs d'évolution du métier

- Au Bénin, le premier texte de loi de référence remonte à 2009.

  Il s'agit de la loi informatique et libertés (Loi N° 2009 - 09 du 22 Mai 2009) qui a instauré la Commission Nationale de l'Informatique et des Libertés (CNIL).

- Afin 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 par la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin qui consacre son livre V à la **protection des données personnelles**.
- Cette dernière a été elle-même modifié par la loi 2020-35 du 06 janvier 2021 apportant une légère modification à la composition et au fonctionnement de l'autorité de contrôle.

1- Contexte et facteurs d'évolution du métier

- Le Code du Numérique vise, d'une part **à simplifier** les formalités de demandes d'avis, de déclaration et d'autorisation auprès de l'autorité de protection des données, et d'autres part **à responsabiliser** davantage les **responsables de traitement (RT)**.

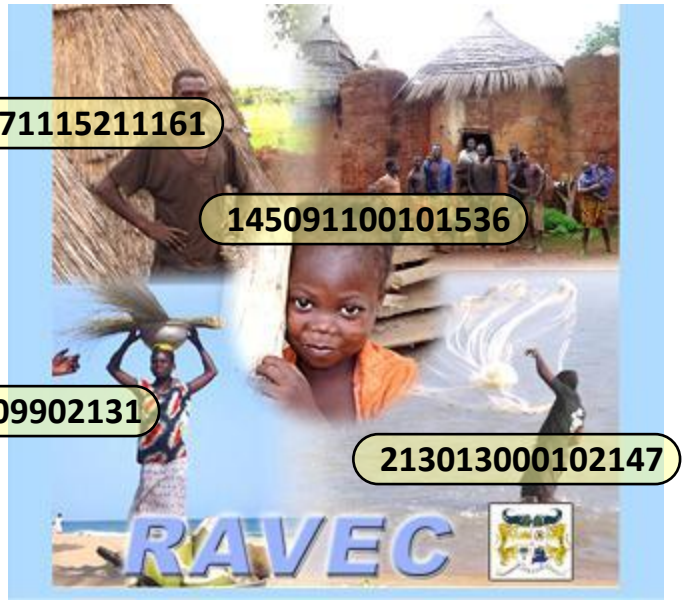
- Ce code **crée une nouvelle fonction** et oblige le responsable de traitement selon le cas à désigner ou non, au sein de leur entreprise un **Délégué à la Protection des Données personnelles (DPDP) pour s'occuper de cette nouvelle fonction.**

- Le Code du Numérique est un texte majeur posant des règles plus strictes relatives au traitement des données à caractère personnel, à la libre circulation de celles-ci, et au respect des droits des personnes (droit à l'information, droit à l'accès, droit d'opposition, …).

2- Genèse de la protection des données au Bénin

La loi sur la protection des données au Bénin tire son origine du Rejet du RAVEC

7 Novembre **2006**



« ***RAVEC : recensement Administratif National à vocation état civil*** **» a pour objectifs:**

- **la collecte de données** relatives à l'état civil des personnes qui viennent de se faire délivrer, en audiences foraines, leur extrait d'acte de naissance ainsi que celles possédant déjà leur acte de naissance ou jugement supplétif;
- **l'attribution à chaque citoyen d'un numéro unique et national d'identification** (N.D.N.I) » ;

Le projet RAVEC

Projet du gouvernement béninois tendant à identifier chaque citoyen par un numéro d'identification a été déclaré contraire à la constitution suite au recours en inconstitutionnalité par le citoyen BOTOKOU Georges, du Décret n° 2006-520 du 15 septembre 2006,

En réponse:

Il a été proposé de créer une « autorité administrative indépendante» pour garantir le développement de l'informatique dans le respect de la vie privée et des libertés sur le modèle français (1978)

2- Genèse de la protection des données au Benin

- Depuis lors les bases juridiques de la protection des données personnelles dans notre pays trouvent leurs origines dans :
  - **La constitution**
  - **La loi N° 2009 - 09 du 22 MAI 2009** modifiée par :
    - ➢ la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin (CDN) et
    - ➢ La loi 2020-35 du 06 janvier 2021 modifiant la loi n° 2017-20 du 20 avril 2018
- Le siège de la protection des données dans le Code du Numérique (CDN) est le livre Vème.
- Ce livre est aujourd'hui le bréviaire et le socle juridique de toutes les activités du DPDP.

3. Définitions

1. Données personnelles
2. Données sensibles
3. Traitement de données personnelles
4. Responsable de traitement
5. Délégué à la protection des données Personnelles (DPDP)

1. Définition d'une donnée à caractère personnel

« ***Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement,*** *par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. ……. »*

Exemples

Groupe sanguin

Nom, Prénom, Adresse, Date de Naissance

N° de téléphone

Numéro de Sécurité Sociale

Photographie

Numéro de dossier client

Race, religion, ethnie,

Adresse IP

casier judiciaire

Plaque d'immatriculation

Adresse E mail

Numéro de Carte Bancaire

Emprunte digitale, vocale

2. Données sensibles

Les données sensibles forment une catégorie particulière des données personnelles.

Les données sensibles sont celles qui **font apparaître**, **directement ou indirectement,** les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci.

Autres données à risque :

- Données génétiques
- Données relatives aux infractions pénales, aux condamnations
- Données comportant des appréciations sur les difficultés sociales des personnes
- Données biométriques
-Données comportant le NIU.

Par principe, la collecte et le traitement de ces données sont interdites.

3. Qu'est-ce qu'un « traitement de données personnelles » ?

Un « traitement de données personnelles » **est une opération**, ou ensemble d'opérations, **portant sur des données personnelles**, quel que soit le procédé utilisé pour la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'extraction, la consultation, la communication par transmission ou diffusion ou toute autre forme de mise à disposition ou de d'exploitation.

C'est donc une notion très large : tout maniement de données, y compris une simple consultation, est un « traitement de données personnelles ».

EXEMPLES DE TRAITEMENTS

Tenue du registre d'état civil, gestion des inscriptions à l'école, tenue du cadastre, gestion de la liste électorale, gestion des ordures ménagères, etc.

Il peut s'agir d'une base de données, d'un fichier papier ou numérique, d'une application mobile, de dispositifs biométriques, de sites web, etc…

4- Le 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** *(désigne qui peut être responsable du traitement)*
  - **qui, seul ou conjointement avec d'autres** (La responsabilité d'un traitement de données peut reposer sur une ou plusieurs personnes d'ou l' idée de co-responsabilité)
  - **prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens (article 1).** *(revient à identifier 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 de contrôle, 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

4- Le Responsable des traitement : Définition

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 donc, d'une part, une personne physique ou morale distincte du responsable du traitement et, d'autre part, une personne physique ou morale qui traite les données à caractère personnel pour le compte du responsable du traitement, sans possibilité de faire quelque traitement que ce soit **sans l'autorisation expresse** du responsable de traitement.

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

- 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.

5. Délégué à la protection des données (DPDP)

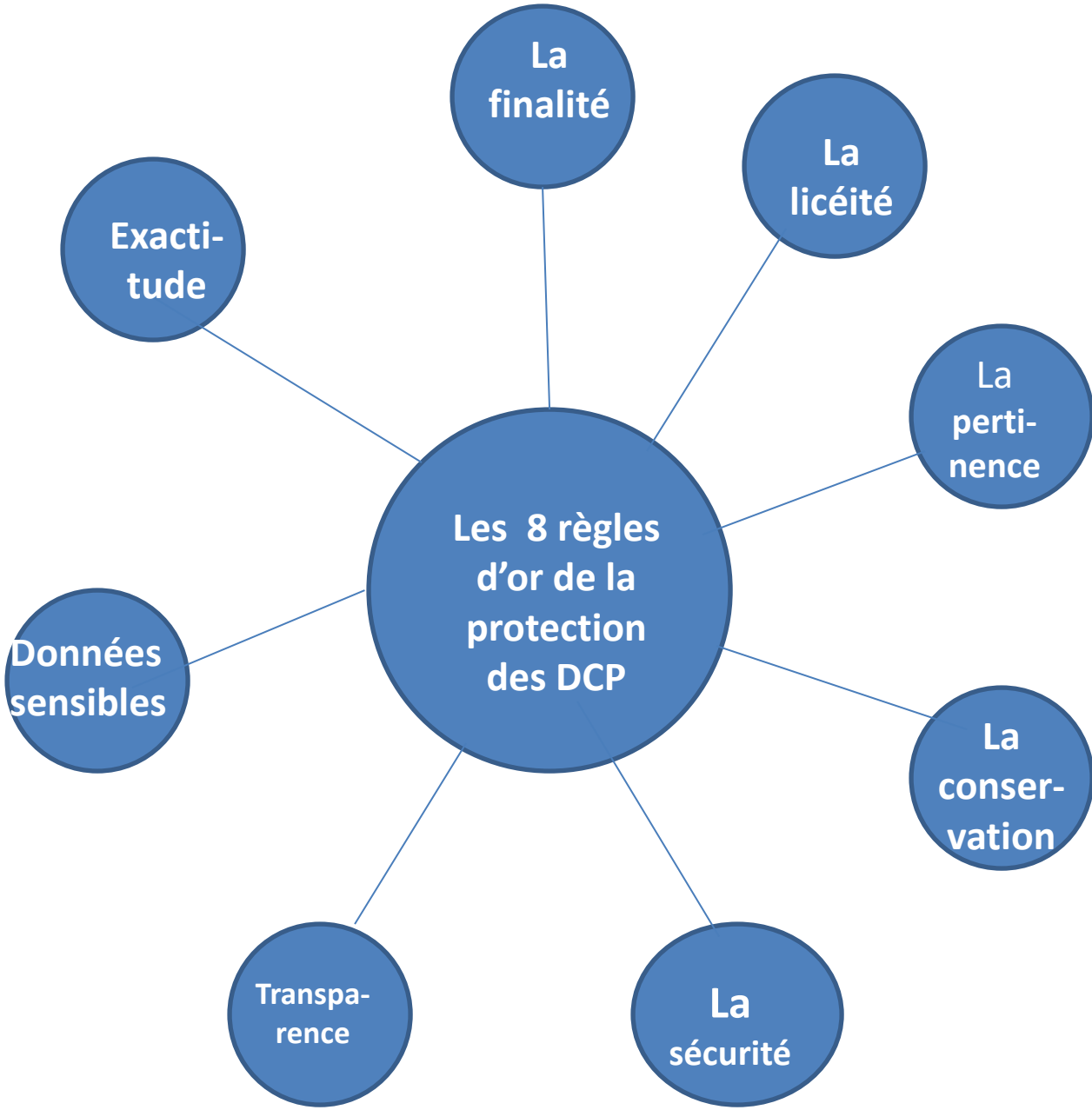
- Le Délégué à la Protection des Données personnelles (DPDP ou DPO pour Data Protection Officer) est le professionnel chargé des différents traitements de données personnelles au sein d'une entreprise.

- Il veille à la protection de ces données personnelles et à leur mise en conformité selon la réglementation en vigueur.

- Agissant comme **un véritable chef d'orchestre**, il est le centre des actions pour assurer la coordination et la gestion des données personnelles.

- En effet, dans le cadre de la mise en œuvre du principe de la responsabilisation des entreprises, le **Code du numérique (CDN) prévoit la désignation, d'un DPDP** en application de l'article **430** du code du numérique.

B. Les grands principes des règles de protection des DCP



B. Les grands principes des règles de protection des DCP

- La loi sur la protection des DCP définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données;
- Chaque traitement de données à caractère personnel doit répondre donc à des conditions; il s'agit entres autres des 8 règles d'or de la protection des données personnelles que nous allons vous présenter:

PRINCIPE 1: Respect de la Finalité

Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation. Autrement dit, il n'est pas permis de collecter des données lorsque l'on ne sait pas quel usage en faire.
En principe, la finalité initiale doit être respectée, afin d'éviter tout « détournement de finalité »

EXEMPLE DE FINALITÉ

Un maire ne pourra pas se servir du fichier des inscriptions scolaires pour faire de la communication politique. La liste électorale pourra en revanche être utilisée à cet effet

TOUT DÉTOURNEMENT DE FINALITÉ EST PASSIBLE DE SANCTIONS PÉNALES.

PRINCIPE 2: Respect de la licéité ou Principe du consentement et de légitimité

Chaque traitement doit être licite.
Cela signifie d'abord qu'il doit être conforme au droit en général

Pour être licite, un traitement doit répondre au moins à l'une des 6 conditions (bases légales) suivantes :

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

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

PRINCIPE 2: Respect de la licéité ou Principe du consentement et de légitimité

Chaque traitement doit être licite.
Cela signifie d'abord qu'il doit être conforme au droit en général

3. La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

4. Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

5. Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

6. Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

PRINCIPE 2: Respect de la licéité ou Principe du consentement et de légitimité

Chaque traitement doit être licite.
Cela signifie d'abord qu'il doit être conforme au droit en général

EXEMPLE DE BASE LÉGALE

La tenue du registre de l'état civil est une obligation légale. Mais, dans le cas de la diffusion des évènements familiaux, les données enregistrées aux fins d'inscription d'un acte sur le registre de l'état civil ne peuvent être utilisées par les élus municipaux pour adresser des félicitations ou des condoléances. De même, ces informations ne peuvent être diffusées (dans la presse ou sur tout autre support) que si les personnes concernées ont, au moment de l'établissement de l'acte, donné leur consentement à ce message personnalisé ou à cette publication

PRINCIPE 2: Respect de la licéité ou Principe du consentement et de légitimité

• Aux termes de l'article **389**, le traitement des DCP est considéré comme légitime si la personne concernée donne son consentement.

• Le consentement est un concept central en ce sens que tout résidant sur le territoire doit avoir donné explicitement son consentement pour que ses DCP puissent être collectées, traitées et conservées.

• Pour appuyer cette exigence, le code restreint la portée du système de consentement explicite. Il stipule que ces données doivent être collectées pour une finalité prédéfinie et très spécifique. Toute personne concernée doit être clairement informée de cette finalité.

• L'exigence de loyauté de ce principe reconnaît à tous les résidents, le « droit à l'oubli », ce qui signifie qu'ils peuvent obtenir sur demande la suppression de leurs DCP de toutes les banques de données du responsable du traitement (et de celles de ses sous-traitants).

PRINCIPE 3: La Pertinence des Données Traitées ou principe de limitation des données

Seules doivent être traitées les informations **pertinentes et nécessaires** au regard des objectifs poursuivis.

Exemple 01 *:*

Le recueil d'informations sur l'entourage familial, l'état de santé ou encore le numéro de sécurité sociale d'un candidat à un recrutement n'est pas pertinent.

Même si le numéro de sécurité sociale peut être parfois nécessaire pour certaines formalités d'embauche…

PRINCIPE 3: La Pertinence des Données Traitées ou principe de limitation des données

EXEMPLE 02

Pour l'inscription à l'école élémentaire, il est légitime de demander un livret de famille, un justificatif de domicile et un document attestant que l'enfant a reçu les vaccinations obligatoires pour son âge.

Lors d'une inscription scolaire, il n'est en revanche pas pertinent de demander le numéro de sécurité sociale du ou des représentants légaux ou encore la copie de leur carte de crédit.

EXEMPLE 03

Pour la gestion de la cantine scolaire, il suffit d'enregistrer uniquement les informations relatives au régime alimentaire et aux aliments à proscrire pour un élève **plutôt que d'inscrire son état de santé** (ex : « diabétique ») ou de mentionner sa religion

PRINCIPE 4: Conservation limitée des données (art.383 et 396)

- **Les données ne peuvent être conservées dans les fichiers de façon indéfinie ; la durée nécessaire doit être établie par rapport à la finalité poursuivie;**

- **Une durée de conservation précise doit être déterminée en fonction de la finalité de chaque fichier.**

Dès que la finalité pour laquelle elles ont été collectées est atteinte, les données selon les cas peuvent être :

- **Archivées,**
- **supprimées ou**
- **anonymisées**

PRINCIPE 4: Conservation limitée des données (art.383 et 396)

. • L'alinéa 6 de l'article 383 prévoit que les données soient << conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées.>>

• Toutefois, Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 396, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par les dispositions du présent Livre afin de garantir les droits et libertés de la personne concernée ;

PRINCIPE 5: Sécurité et Confidentialité (art. 383)

L'employeur, en tant que responsable du traitement, est astreint à une obligation de sécurité adaptée à la nature des données et aux risques présentés par le traitement :

- il doit empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès (intrusion);
- il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés.

Exemples

- ***chaque salarié doit disposer d'un mot de passe individuel régulièrement mis à jour.***
- ***Les droits d'accès aux données doivent être précisément définis en fonction des besoins réels de chaque personne (lecture, écriture, suppression)***
- ***Il peut également être utile de prévoir un mécanisme de verrouillage systématique des postes informatiques au-delà d'une courte période de veille***
- **chiffrement des données sur internet**

PRINCIPE 5: Sécurité et Confidentialité (art. 383)

L’alinéa **7** de l'article **383** prévoit que les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

PRINCIPE 5: Sécurité et Confidentialité (art. 383)

EXEMPLE

Dans le cadre des demandes d'actes d'état civil, l'accès aux informations nécessaires à l'instruction de ces demandes doit être limité aux seuls agents chargés de cette activité.

Les données peuvent néanmoins être communiquées à des tiers autorisés à cet effet, en application de dispositions législatives particulières (Inspections du travail, services fiscaux, services de police…).

PRINCIPE 6: Transparence (art 384)

Aux termes de l'article 384, le principe de transparence implique une information obligatoire et claire ainsi qu'intelligible de la part du responsable du traitement portant sur les données à caractère personnel.

Les personnes doivent être informées de l'utilisation des données les concernant et de la manière dont ils peuvent exercer leurs droits.

PRINCIPE 6: Transparence (art 384)

Principe général de transparence
Le Code du Numérique introduit **un principe général de transparence** en vertu duquel toute communication à l'intention d'un individu, y compris dans le cadre de l'exercice de ses droits, doit être réalisé d'une façon « concise, transparente, compréhensible et aisément accessible » et en des termes « clairs et simples ».

Le responsable du traitement doit répondre à une personne exerçant ses droits « dans les meilleurs délais et en tout état de cause dans **un délai d'un mois à compter de la réception de la demande** ». Ce délai peut être **prorogé de deux mois « compte tenu de la complexité et du nombre de demandes ».** L'organisme devra cependant informer le requérant de cette prorogation et des motifs de ce report dans le délai initial d'un mois. ».

Aucun paiement ne doit être exigé en contrepartie de l'exercice de ces droits. Si le responsable de traitement juge les demandes « manifestement infondées ou excessives, notamment en raison de leur caractère répétitif », il peut refuser d'y donner suite ou facturer la réalisation des demandes.
Les informations doivent être fournies à la personne « par écrit ou par d'autres moyens y compris lorsque c'est approprié par voie électronique ». Si la demande est exprimée par voie électronique, il y sera répondu de préférence par voie électronique.

Il importe au préalable de vérifier l'identité de la personne.

PRINCIPE 7: Protection particulière des données sensibles

Les données sensibles ne peuvent être collectées et traitées que dans certaines conditions.

PRINCIPE 7: Protection particulière des données sensibles

Le traitement des données sensibles est en principe interdit.
C'est-à-dire qu'il est interdit de recueillir et d'utiliser ces données.

Ces dernières jouissent d'une protection plus accrue, parce que leur traitement présente un risque plus important pour les droits et libertés des personnes concernées.

Cette interdiction de principe s'applique même dans le cadre de traitements temporaires (conservation temporaire, enregistrement temporaire, extraction temporaire…). ces dernières jouissent d'une protection plus accrue,

Cependant, les données sensibles peuvent être collectées et traitées dans certaines conditions exceptionnelles.

PRINCIPE 7: Protection particulière des données sensibles

Les exceptions au principe d'interdiction du traitement des données sensibles

Le traitement des **données sensibles** est autorisé :

1. Si la personne concernée a donné son consentement exprès. Ce consentement doit être écrit et la personne doit avoir été informée au préalable. En outre, le responsable du traitement doit pouvoir en apporter la preuve ;

2. Si le traitement est indispensable à l'exécution des obligations ou des droits propres au responsable du traitement ou à la personne concernée pour les matières liées au droit du travail, la sécurité sociale et la protection sociale

3. Si le traitement est nécessaire pour la sauvegarde de la vie de la personne concernée ou d'une autre personne, surtout dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

PRINCIPE 7: Protection particulière des données sensibles

Les exceptions au principe d'interdiction du traitement des données sensibles

Le traitement des **données sensibles** est autorisé :

4. Si les traitements concernent les membres et adhérents d'une fondation, de tout organisme à but non lucratif ou une association ethnique, religieuse, politique, philosophique ou syndicale ;

5. Si les données ont été rendues publiques par la personne concernée ;

6. Si les données sont nécessaires à la contestation ou à la défense d'un droit devant la justice ;

7. Si l'utilisation des données présente un intérêt public important et autorisé par la **APDP** ;

PRINCIPE 7: Protection particulière des données sensibles

Les exceptions au principe d'interdiction du traitement des données sensibles

Le traitement des **données sensibles** est autorisé :

8. Lorsque le traitement est nécessaire pour la médecine préventive ou du travail et concerne directement la capacité d'une personne à travailler, les diagnostics médicaux, la prise en charge sociale, la prise en charge sanitaire ou la gestion des systèmes et des services de santé ou de protection sociale ;

9. Lorsque le traitement est justifié par des motifs d'intérêt public dans le domaine de la santé publique (protection contre les menaces sanitaires transfrontalières, garantir des normes élevées de qualité et de sécurité de soins de santé…) ;

10. Si le traitement présente un intérêt public à des fins de recherches historiques, scientifiques ou statistiques.

PRINCIPE 8: Le principe d'exactitude (art 383)

Le principe d'exactitude est étroitement lié à celui de transparence.

Il prescrit à l'alinéa 5 de l'article 383 que les données doivent être exactes et, si nécessaire, mises à jour.

Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées .

PRINCIPE 8: Le principe d'exactitude (art 383)

Le principe d'exactitude est étroitement lié à celui de transparence.

Il prescrit à l'alinéa 5 de l'article 383 que les données doivent être exactes et, si nécessaire, mises à jour.

Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées .

D. Profil de poste du DPDP: Son rôle et ses missions

1. Rôle du DPDP
2. Missions du DPDP

I. Rôle du DPDP

- **Dans le cadre de la mise en œuvre du principe de la responsabilisation des entreprises, le code du numérique prévoit la désignation, d'un Délégué à la Protection des Données (DPD ou DPO pour Data Protection Officer) en application de l'article 430 du code du numérique.**
- **Le DPDP est le professionnel chargé des différents traitements de données personnelles au sein d'une entreprise, d'une collectivité…..**
- **Il veille à la protection de ces données personnelles et à leur mise en conformité selon la réglementation en vigueur.**
- **Agissant comme un véritable chef d'orchestre, il est le centre des actions pour assurer la coordination et la gestion des données.**

I. Rôle du DPDP

- **Le DPD joue en général un rôle clé dans la promotion d'une culture de la protection des données au sein de l'organisme et de manière spécifique il contribue à mettre en œuvre entre autres des éléments essentiels tels que :**

  - ✓ ***les principes relatifs au traitement des données personnelles,***
  - ✓ ***les droits des personnes concernées par un traitement,***
  - ✓ ***la protection des données dès la conception et la protection des données par défaut, (culture des principes de Privacy by Design et de Privacy by Default au sein de l'organisme)***
  - ✓ ***la tenue du registre des activités de traitement,***
  - ✓ ***la sécurité du traitement ainsi que***
  - ✓ ***la notification et la communication des violations de données.***

I. Rôle du DPDP

- Son rôle fondamental est de veiller à la mise en conformité de l'ensemble des traitements dans l'organisme avec les prescriptions de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

- Par conséquent, le délégué apparaît comme
  - ✓ ***le gardien des données personnelles au sein de l'organisme ou***
  - ✓ ***l'APDP en miniature au sein de l'organisme*.**

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

- Les missions du délégué à la protection des données sont au moins les suivantes :
  - ✓ *Informer et conseiller l'organisme*
  - ✓ *Contrôler la conformité*
  - ✓ *Coopérer avec l'Autorité de Protection des Données Personnelles (APDP)*
  - ✓ *faire office de point focal pour l'Autorité sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 412, et mener des consultations, le cas échéant, sur tout autre sujet;*
  - ✓ *…etc.*

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

2.1. Informer et conseiller l'organisme

Le délégué a vocation à diffuser une culture de la protection des données au sein de l'organisme.

- Il doit communiquer sur les règles applicables, et sur les moyens de s'y conformer, à la fois auprès:
  - ✓ du représentant légal de l'organisme (Secrétaire Exécutif des Mairies au Bénin, Président de l'**E**tablissement **P**ublic de **C**oopération **I**ntercommunale, DG, Ministre etc.),
  - ✓ du responsable de la conformité des traitements déployés par rapport aux cahiers des charges, et
  - ✓ des services opérationnels chargés de leur mise en œuvre.

- Il les conseille par exemple sur la réalisation d'une analyse d'impact relative à la protection des données : obligation ou non d'y procéder, méthodologie à suivre, mesures/garanties techniques et organisationnelles à prévoir, nécessité ou non de consulter l'APDP.

II. Les missions du délégué à la protection des données

(Artide432 du code du numérique)

- **2.1 Informer et conseiller la collectivité (suite)**

Il existe différents modes d'intervention possibles pour le délégué :

- animation de séances d'information « CDN »,
- recours à différents outils de communication (affiches, rubrique spécifique sur l'intranet, etc.) ;
- établissement de modèles de mentions d'information et de clauses contractuelles encadrant la sous-traitance ;
- formalisation de politiques de confidentialité des données, de procédures relatives à la détection,
- prise en charge et notification des violation de données,
- gestion des demandes d'exercice des droits Informatique et Libertés,
- etc.

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

2.2 Contrôler la conformité

- **Le Délégué contrôle le respect** de la loi en matière de protection des données personnelles, notamment au niveau des finalités des traitements mis en place et du respect des droits des personnes concernées.
- L'une des fonctions principales du DPDP étant d'assurer la mise en conformité de l'organisme ou de la collectivité à la loi, il peut, en appui au Responsable de traitement ou au sous-traitant, participer aux missions suivantes :
  - ✓ *Cartographier les traitements de données effectués par l'organisme*
  - ✓ *Participer à l'établissement des règles internes en matière de protection des données*
  - ✓ *Recenser l'ensemble des activités de traitement mises en œuvre par l'organisme*
- Afin d'assurer ces dernières, la loi prévoit la mise en place de divers outils dont la tenue du registre des activités de traitement de l'entreprise

II. Les missions du délégué à la protection des données

(Artide 432 du code du numérique)

- **2.2 Contrôler la conformité (suite)**
- Dans la majorité des cas, le délégué tient et actualise le registre des traitements.
- Le registre lui offrira une vue d'ensemble sur les finalités et conditions d'utilisation des données :
  - quels objectifs,
  - quelles informations,
  - quels destinataires,
  - quelle durée de conservation,
  - quelles mesures de sécurité, etc. ?

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

- **2.2 Contrôler la conformité (suite)**

Pour chacun des traitements mentionnés dans le registre, le délégué vérifie qu'**ils disposent d'une base juridique:**

- *répondent à une obligation légale,*
- *répondent à une mission d'intérêt public, etc.* ***et***
- **satisfont bien aux grands principes de protection des données tels que :**

✓ *la transparence,*
✓ *La confidentialité des données,*
✓ *Le respect des droits des personnes, etc.).*

II. Les missions du délégué à la protection des données

(Artide 432 du code du numérique)

2. Contrôler la conformité (suite)

- Le **registre est à géométrie variable**, selon la taille de la structure et la nature de ses activités. Celui des petites communes pourra contenir moins d'une dizaine de fiches(gestion de l'état civil, de la liste électorale, du cadastre, appui aux populations indigentes et aux seniors, des prêts de la bibliothèque communale, etc.).
- Le délégué doit concentrer prioritairement ses efforts sur :
  - les traitements qui présentent des risques particuliers (sensibilité des données en cause ou de la finalité, portée du traitement, insuffisance évidente des mesures de sécurité, etc.).
  - Les personnels à former,
  - Les vérifications à mener,
  - Les plans d'actions correctives à actionner

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

2.2 Contrôler la conformité (suite)

Attention :

Le délégué n'est pas personnellement comptable du respect de la règlementation.

Ainsi, en cas de manquement aux obligations en cause, il ne pourra être tenu juridiquement responsable en lieu et place de la structure et de son représentant légal.

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

2.3 Être le point de contact pour les personnes dont les données sont traitées et l'interlocuteur privilégié de l'APDP

Les personnes concernées par les traitements de l'organisme (usagers et agents en particulier), peuvent soumettre au délégué toute question relative au traitement de leurs données.

Il appartient également au délégué de veiller à ce qu'il soit répondu aux demandes d'exercice des droits (accès, rectification, opposition, etc.) dans les délais prévus par les textes.

II. Les missions du délégué à la protection des données

(Article 32 du code du numérique)

2.3. Être le point de contact pour les personnes dont les données sont traitées et l'interlocuteur privilégié de l'APDP

- Le délégué joue par ailleurs un **rôle de « facilitateur » dans les relations entre l'organisme et l'APDP** : il doit coopérer avec elle et permettre son accès aux documents et informations sollicités dans l'exécution de ses missions (contrôles sur place/sur pièces, instruction de plaintes, notifications de violations de données, etc.).

II. Les missions du délégué à la protection des données

(Article 432 du code du numérique)

2.3. Être le point de contact pour les personnes dont les données sont traitées et l'interlocuteur privilégié de l'APDP

- **Pour que l'accès au délégué soit au maximum facilité, la collectivité doit mentionner les moyens de le contacter sur ses différents formulaires de collecte de données, ainsi que sur son site internet**

  (ex. : adresse électronique dédiée, telle que « DPDP@mairieportonovo.bj »).

D. Modalités de désignation et mise en place

1. Nécessité de désigner un DPDP
2. La responsabilité du DPDP
3. Le statut du DPDP dans un organisme
4. Les différentes catégories de DPDP
5. Les compétences
6. Aptitude professionnelle du DPDP
7. La déontologie du DPO

II– La responsabilité du DPDP

- En cas de non-conformité de l'entreprise au CDN, **la responsabilité** du DPDP ne peut pas être **directement** engagée.
- **Attention** : Le **transfert de responsabilité** du responsable de traitement au DPDP **est interdit**.

- Le DPDP ne dispose pas de pouvoir décisionnel concernant la finalité et les moyens du traitement des données personnelles.

- Il est **indépendant** du reste du personnel de l'entreprise. Par conséquent, le responsable de traitement ou les sous-traitants ne peuvent pas le relever de ses fonctions.

- **Bon à savoir** : Le DPDP peut voir sa **responsabilité pénale** engagée en cas de violation intentionnelle d'une des dispositions pénales du CDN.

III - Le statut du DPDP dans un organisme

Le délégué doit :

- **pouvoir rendre compte au niveau le plus élevé de la hiérarchie**

  Quelle que soit sa position précise dans l'organigramme, le délégué désigné en interne doit pouvoir disposer d'un accès direct au niveau exécutif de l'organisme

- **être en mesure d'exercer ses missions en toute indépendance**

  Cette deuxième condition signifie que le délégué bénéficie d'une liberté dans les analyses et actions qu'il décide d'entreprendre, et qu'il ne doit pas recevoir d'instruction dans l'exercice même de ses missions (par exemple, sur le sens des avis qu'il rend, sur l'orientation des conseils qu'il donne, etc.).

- **être à l'abri des conflits d'intérêts**

  La condition relative au conflit d'intérêts – ne pas se retrouver à la fois juge et partie – constitue une garantie d'indépendance importante. Ainsi, lorsque le délégué est amené à exercer d'autres fonctions de façon concomitante, elles ne doivent pas le conduire à décider des finalités et/ou des moyens de mise en œuvre des traitements de données personnelles..

IV - Les différentes catégories de DPDP

1. Le délégué interne
2. Le délégué externe
3. Le délégué mutualisé
4. Le délégué aux multifonctions

IV – Les différentes catégories de DPDP :

DPDP interne

• Le DPO peut être un employé de l'organisme.

• Il peut être affecté, en fonction de l'importance de la structure, à temps plein ou à temps partiel.

• Ce qui est primordial c'est qu'il soit bien identifié, qu'il est le temps nécessaire pour accomplir sa mission.

• Un délégué interne présente l'avantage de bien connaître la structure, de s'investir, a priori, sur le moyen ou long terme. Par contre dans les petites structures la mission de délégué à la protection des données peut être considérée comme annexe et la formation peut parfois être insuffisante.

• Le DPO doit avoir un positionnement hiérarchique suffisant pour qu'il ait une autorité suffisante.

• L'indépendance du délégué interne peut être difficile à respecter si ce dernier n'est pas fermement soutenu par la direction générale.

IV- Les différentes catégories de DPDP :

DPDP externalisé

- Les organisations publiques ou privées peuvent également confier les mission de DPDP à des consultants extérieurs dans le cadre de contrat de prestation de services.

- L'externalisation présente l'avantage d'avoir affaire à un professionnel spécialisé dans ce domaine.

- Le délégué externe est assuré, ce qui peut présenter un avantage pour l'organisme pour qui il travaille qui pourra se retourner vers lui en cas d'amende si le délégué est responsable de la faute commise.

- Par exemple si le délégué n'a pas informé correctement des règles à suivre et des sanctions encourues, sa responsabilité pourra être engagée.
  A contrario si le délégué a conseillé une analyse d'impact au responsable de traitement et que celui-ci n'y donne pas suite pour des raisons qui lui appartiennent, la responsabilité du DPDP externe ne sera pas engagée.

- Le recours à un DPDP externe ne dispense cependant pas l'Organisme de désigner un correspondant interne qui sera le référent du délégué dans le cadre de l'exercice de sa mission. **Ceci est fortement conseillé.**

IV - Les différentes catégories de DPDP :

DPDP mutualisé

- Le DPO qu'il soit interne ou externe peut être mutualisé entre plusieurs organisations.

- C'est souvent le cas pour les communes qui mutualisent les postes de DPDP avec l'établissement public de coopération intercommunale (EPCI) auquel elles appartiennent. Il convient de bien déterminer la nature des tâches et le temps passé pour chaque collectivité du DPO mutualisé.

- Il est également important dans ce cas que le délégué soit bien identifié dans chaque structure ou il intervient.

- Il est indispensable que dans chacune d'entre elles il y ait un correspondant avec qui il puisse travailler.

IV - Les différentes catégories de DPDP :

DPDP aux multiples fonctions

- A l'intérieur même de l'organisme le DPDP peut exercer des fonctions mutualisées.

- C'est ainsi qu'un DPDP pourra être en même temps responsable qualité.

- Mais il faut faire attention à ce que de multiples attributions à un DPO en plus de la protection des données personnelles ne génèrent pas de **conflit d'intérêt** comme ce pourrait être le cas si le DPDP était en même temps chargé de la sécurité informatique.

-

IV - Les différentes catégories de DPDP :

- **Mutualisation :** Une solution adaptée à la situation des plus pétites entreprises

La mutualisation du délégué permet en effet de ***rationaliser les coûts associés à la fonction,***

tout en bénéficiant de services de qualité*, dispensés par des professionnels disposant de compétences Informatiques et Libertés, de la connaissance des problématiques propres au secteur public local, d'une proximité avec les élus et de la disponibilité nécessaires à un exercice efficace des missions.*

- **La convention de mutualisation et les garanties à prévoir**

Les collectivités territoriales, établissements publics locaux et organismes privés chargés d'une mission de service public qui optent pour la mutualisation doivent conclure une

convention définissant les conditions dans lesquelles s'exerce cette mutualisation.

V - Les compétences

Le DPO doit connaître parfaitement le CDN, mais aussi connaître le fonctionnement de l'organisme duquel il a en charge la protection des données ou tout du moins en comprendre rapidement les grands principes de fonctionnement.

Ainsi, les **compétences techniques** ci-après sont **requises:**

- Compétences juridiques : maîtrise du cadre légal
- Compétences informatiques : connaissance des systèmes d'information (protocole de communication, base de données, cloud, cookies, etc.), connaissances dans le domaine de la sécurité informatique (chiffrement, authentification forte, traçabilité, menaces, plan de continuité et de reprise d'activité, tests de pénétration, etc.)
- Savoir réaliser une analyse d'impact, rédiger des mentions d'information, gérer une violation de données, etc.
- Bonne connaissance de l'organisation et du fonctionnement de la structure
- Solides connaissances des techniques de gestion de projet (expression des besoins, planning, cahiers des charges, etc.) et des différents outils associés

V - Les compétences

- **Le délégué doit donc être choisi sur la base de ses connaissances du droit et de ses pratiques en matière de protection des données.**

Toutefois, le CDN n'impose pas aux organismes de recourir à un profil particulier : aucun agrément n'est prévu, aucune exigence de diplôme ou condition statutaire n'est fixée.

- **Il peut donc s'agir d'une personne, physique ou morale, issue du secteur juridique, technique (informatique) ou de tout autre secteur (archives, communication, qualité, etc.), interne ou externe à l'organisme.**

VI - Aptitude professionnelle du DPO

- Adaptabilité
- Aisance relationnelle
- Autonomie
- Capacité d'adaptation
- Capacité rédactionnelle
- Curiosité sectorielle et goût pour l'innovation
- Esprit d'initiative
- Esprit de synthèse et d'analyse
- Éthique
- Force de proposition et de conviction
- Organisation
- Pédagogie
- Polyvalence
- Rigueur
- Sens de l'écoute et de la communication
- Sens des délais et des résultats

VII - La déontologie du DPO

- Le DPO doit être **libre** et **indépendant** dans l'exercice de sa mission.

- Il doit avoir les **moyens** adaptés.

  Il ne peut être une simple fonction sur le papier, sans moyen d'agir.

- Il doit être à l'abri des **conflits d'intérêt**, notamment vis-à-vis de ses autres activités.

- Des associations professionnelles de DPO éditent des chartes de déontologie. Il est utile de s'y référer voire d'y adhérer.

CONCLUSION

Devant garantir tant la confidentialité que l'intégrité de ces données, les entreprises sont désormais tenues de mettre en place des techniques de sécurisation des données et de procéder à des audits réguliers de leurs systèmes informatiques et des procédures en matière de traitement des données. Elles ont enfin comme obligation de définir des procédures permettant la mise en place de solutions correctives, le cas échéant, la non-conformité pouvant entraîner de lourdes pénalités.

Annexes:

i. Lu pour vous : Une étude sur le métier de DPDP