AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES
(APDP)

FORMATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES PERSONNELLES

Thème : ***Protection des données personnelles au Bénin et les grands principes de la protection des données***

Intervenant : Professeur ZANNOU Martial Tiburce

Novembre 2021

Sommaire

I/ Introduction à la protection des données personnelles

A.Sources, fondements et notions

B.Champ d’application

- II/ les principes de la PDP

I/ Introduction à la protection des données personnelles

A.Sources, fondements et notions

1)Les sources

Les bases juridiques de la protection des données personnelles trouvent leurs

origines dans les sources nationales et internationales.

- ***Sources nationales***

- Au Bénin, la protection des données à caractère personnel est réglementée dans:

➢ *La constitution*

➢ la loi N° 2009 - 09 du 27 Avril 2009 modifiée par la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin et la loi 2020-35 du 06 janvier 2021.

Ce code du numérique a pour objet de régir :

- les activités qui relèvent des réseaux et services de communications électroniques ;
- les outils électroniques ;
- les services de confiance en l'économie numérique ;
- le commerce électronique ;
- la protection des données à caractère personnel ; et
- la cybercriminalité et la cybersécurité

Le siège de la protection des données est le livre V^{ième}. Ce livre est le bréviaire et le socle juridique de toutes les activités relatives à la protection des données. Il fixe un cadre légal de protection de la vie privée et professionnelle consécutif à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel.

Il convient de savoir quelles sont les données personnelles à protéger. La notion de donnée à caractère personnelle en particulier et celle de données en général, est abondamment évoquée dans le code qui y a apporté une clarification conceptuelle.

On entend par :

- - **Données à caractère personnel** : toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée. Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel un prénom ou 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, culturelle, sociale ou économique ;

- **Données afférentes à la création de signature** : les données uniques telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique sécurisée ;

- - **Données biométriques** : toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques

- **- Données concernant la santé** : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

- - **Données de création de cachet électronique** : les données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

- **- Données d'identification personnelle** : l'ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

- - **Données génétiques** : toute information concernant les caractères génétiques héréditaires ou acquis d'une personne physique qui donnent des indications uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;

- - **Données informatiques** : toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

- - **Données relatives aux abonnés** : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

- ▪ le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

- ▪ l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

- ▪ toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;

- - **Données relatives au contenu** : contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication. Il s'agit de tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic ;
- - **Données relatives au trafic** : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent;
- - **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 ;
- ***Tout l'enjeu de la protection des personnes*** est de tenter de donner à l'individu un contrôle sur la collecte et l'exploitation de ses données personnelles, même s'il s'agit d'un combat difficile, compte-tenu de la croissance exponentielle des moyens informatiques de collecte et de traitement mondialisés.
- En créant un environnement qui place la protection des données au cœur des entreprises, et protège la capacité des personnes à contrôler leurs données, les entreprises pourront regagner la confiance des clients. Ceci peut être un avantage important pour attirer de nouveaux clients et retenir la clientèle existante.

- **Sources internationales**

- On distingue :

- La résolution A/RES/45/95 du 14 décembre 1990 sur les « *principes directeurs pour la réglementation des fichiers personnels informatisés* »

- **La convention** de l'Union **Africaine** sur la cyber-sécurité et la **protection des données** à caractère personnel, adoptée le 27 juin 2014 à Malabo, en Guinée Equatoriale

- L'Acte additionnel de la CEDEAO relatif à la protection des données à caractère personnel, adopté le 16 février 2010, d'application directe dans les Etats membres de la communauté.

B. Champ d'application

- Le champ d'application d'une loi est la détermination des limites dans lesquelles cette loi s'applique. Le champ d'application du code (évoqué plus haut) est large mais puisqu'il s'agit de protection des données, nous nous y intéresserons spécifiquement. On distingue le champ d'application matériel et le champ d'application territorial.

1)Le champ d’application matériel et territorial

- **Champ d’application matériel**

•Dans le jargon juridique fortement emprunt des expressions latines, l’expression "Ratione materiae" signifie "en raison des dispositions légales ou règlementaires qui règlent la matière »

•La notion de compétence matérielle recouvre toutes les classes d’affaires dont un tribunal peut connaître. En d’autres termes, il s’agit de la compétence « s’appréciant en raison de l’objet du litige ». Chaque tribunal peut entendre une classe particulière d’affaires : des affaires liées à des litiges de droit du travail ; des affaires liées à l’interprétation ou à la violation de la constitution ; des affaires touchant au droit civil.

- Sachant que le livre V^{ième} régit la matière de protection des données personnelles, l’article 380 abonde dans le même sens et précise que les dispositions du livre V^{ième} s’appliquent notamment à :

- 1- toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation de données à caractère personnel par une personne physique, par l’État, les collectivités locales, les personnes morales de droit public ou de droit privé ;

- 2- tout traitement automatisé en tout ou en partie, ainsi que tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l’exception des traitements visés à l’alinéa 2 ;

3- tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d’infractions pénales ou la sûreté et les intérêts essentiels de l’État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d’autres textes de loi en vigueur.

•*Champ d’application territorial de la loi*

•L'expression latine "ratione loci" signifie " en raison du lieu". Elle est employée dans les affaires dans lesquelles est soulevée un moyen portant sur la compétence géographique d'une juridiction

•Aux termes de l’article 381, les dispositions du Livre Vième s'appliquent au traitement des données à caractère personnel effectué dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant sur le territoire de la République du Bénin, que **le traitement ait lieu ou non en République du Bénin.**

Les dispositions du livre s'appliquent au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de la République du Bénin par un responsable du traitement ou un sous-traitant qui n'est pas établi en République du Bénin, lorsque les activités de traitement sont liées :

•1- à l'offre de biens ou de services à ces personnes concernées en République du Bénin, qu'un paiement soit exigé ou non desdites personnes ; ou

•2- au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de la République du Bénin ;

•3- le traitement est mis en œuvre sur le territoire d’un Etat membre de la CEDEAO.

2) Les Exclusions

- Les dispositions du Livre Vième ne s’appliquent pas aux traitements de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques lorsque ces données ne sont pas destinées à une communication à des tiers ou à la diffusion.
- Ces dispositions ne peuvent restreindre :
- 1- des modes de production d'informations disponibles en vertu d'une loi pour une partie dans quelque procédure judiciaire que ce soit ;
- 2- le pouvoir des cours et tribunaux judiciaires de contraindre un témoin à témoigner ou de contraindre à la production de preuves

- II/ les principes de la PDP

- La transformation numérique modifie notre façon de travailler. De plus en plus, les équipes de marketing incitent les clients à interagir avec l'entreprise par la voie numérique au travers des médias sociaux et des applications mobiles, en plus des canaux de communication plus traditionnels comme Internet et la messagerie électronique. À mesure que la quantité d'informations partagées par les clients via les nouveaux canaux numériques augmente et que les applications d'entreprise qui traitent des données personnelles se déplacent vers le cloud, le risque de vol ou de fuite de ces données s'accroît. L'un des objectifs premiers du code du numérique est de réduire ce risque.

- Avant de prendre des mesures pour parvenir à une totale conformité, les entreprises doivent faire en sorte de parfaitement comprendre les exigences qu'il fixe. Fondé sur les principes généralement reconnus en matière de protection de la vie privée, le code du numérique énonce dix principes fondamentaux :

- A/ ***<u>Les principes de licéité et de loyauté des traitements</u>***

-
- Aux termes de l’article 383, les données à caractère personnel doivent être :
- 1- traitées légitimement ;
- 2- collectées, enregistrées, traitées, stockées et transmises de manière licite, loyale, transparente et non frauduleuse ;
- 4- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

- ***B/ <u>Principe du consentement et de légitimité</u>***

- Aux termes de l'article 389, le traitement des données à caractère personnel 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 données à caractère personnel 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. Redonner au citoyen le contrôle de ses données.

- 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 données à caractère personnel de toutes les banques de données du responsable du traitement (et de celles de ses sous-traitants).

- Quant à l’obligation de transparence, elle confère à chaque résident le « droit d’accéder » à toutes les données personnelles le concernant détenues par le responsable du traitement. La personne concernée peut demander une copie de toutes ses données dans un format numérique, structuré et couramment utilisé, et sa demande devra être satisfaite dans le mois qui suit sa réception.

- ***Portée du principe du consentement***

- Toutefois, il peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire :

- 1- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

- 2- 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 ou le tiers auquel les données sont communiquées ;

- 3- à l’exécution d’un contrat auquel la personne concernée est partie ou à l’exécution de mesures précontractuelles prises à sa demande ;

- 4- à la sauvegarde de l’intérêt ou des droits fondamentaux ou à l’intimité de la vie privée physique concernée.

- Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

•1- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;

•2- du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;

•3- de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 395 et si ce n'est pas le cas

•4- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;

•5- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

C/ la prospection commerciale

- La prospection commerciale est un outil indispensable pour l'entreprise. Omniprésente auprès des consommateurs, elle n'en reste pas moins importante auprès des professionnels. Dans un contexte d'économie numérique, comment prospecter en toute conformité ?

• C-1) *L'encadrement de la prospection commerciale*

- Les règles en matière de prospection commerciale consacrent le principe du recueil du consentement préalablement à toute prospection commerciale par voie électronique (e-mail, SMS et fax)

- La personne concernée doit alors donner son consentement pour la prospection commerciale au moment de la collecte de ses données personnelles. Le recueil du consentement est souvent matérialisé par une mention du type **« En cochant cette case, vous acceptez de recevoir des propositions commerciales par voie électronique »**.

- Le recours aux cases pré-cochées est à proscrire, puisque le consentement doit être univoque, c'est-à-dire qu'il doit résulter d'un acte positif. De plus, le consentement ne vaut que pour la personne pour laquelle il est recueilli.

- Le code du numérique prône la transparence : si les données de la personne concernée sont susceptibles d'être transmises ou cédées à des partenaires, elle devra en être informée au préalable.

- Pour être valable, le consentement doit être spécifique, c’est-à-dire donné pour une finalité spécifique (un objectif donné), il faudra donc prévoir une autre case à cocher pour la transmission à des tiers (le consentement doit être donné pour chacune des finalités de la collecte). Il n’est pas possible d’utiliser les données recueillies aux fins de prospection pour une autre finalité.
-

- **C-2) *<u>Dérogation à la prospection commerciale : le droit d’opposition</u>***

- Toute personne physique a le droit de s'opposer, à tout moment, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.
- Elle a le droit, d’une part, d’être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection notamment commerciale, caritative ou politique et, d’autre part, de se voir expressément offrir le droit de s’opposer, gratuitement, à ladite communication ou utilisation.
- Ce droit doit être explicitement proposé à la personne concernée d'une façon intelligible et doit pouvoir être clairement distingué d'autres informations.

- Lorsqu'il est fait droit à une opposition conformément à cet article, le responsable du traitement n'utilise ni ne traite plus les données à caractère personnel concernées.
- Lorsque les données à caractère personnel sont collectées à des fins de prospection notamment commerciale, caritative ou politique, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant.
- Pour exercer son droit d'opposition, l'intéressé adresse une demande datée et signée, par voie postale ou électronique, au responsable du traitement ou son représentant. Le responsable du traitement doit communiquer dans les trente (30) jours qui suivent la réception de la demande prévue à l'alinéa précédent, quelle suite il a donnée à la demande de la personne concernée.
- Lorsque des données à caractère personnel sont collectées par écrit, que ce soit sur un support papier, support électronique ou tout autre support équivalent, auprès de la personne concernée, le responsable du traitement demande, à celle-ci, sur le document grâce auquel il collecte ses données, si elle souhaite exercer le droit d'opposition.

- Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, autrement que par écrit, le responsable du traitement demande à celle-ci si elle souhaite exercer le droit d'opposition, soit sur un document qu'il lui communique à cette fin au plus tard soixante (60) jours après la collecte des données à caractère personnel, soit par tout moyen technique qui permet de conserver la preuve que la personne concernée a eu la possibilité d'exercer son droit.

- En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d’accès sauf lorsqu’il est établi que les données contestées ont été communiquées par l’intéressé ou avec son accord

- ***D/ <u>Le principe de transparence</u>***

- 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.

- **E/ <u>Le *Principe de confidentialité et de sécurité*</u>**

- Aux termes de l’article 385, les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

- ***F/ <u>Le principe de finalité</u>***

-

- Le principe de limitation des finalités établit, d'une part, que les données à caractère personnel peuvent être traitées pour la ou les finalités prévues initialement uniquement et, d'autre part, que tout traitement ultérieur des données collectées est interdit sans un nouveau consentement de la personne concernée

-

- L'alinéa 3 de l'article 383 rappelle que les données doivent être << collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l’intéressé et des dispositions légales et réglementaires applicables ; >>

- ***G/ <u>Le principe d'exactitude</u>***

- 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 ;

- ***H/ <u>Le principe de conservation limitée des données</u>***

- Les données ne peuvent être conservées que pour une durée prédéfinie et limitée ; la finalité du traitement détermine la durée de conservation. A l'issue du traitement, les données sont soit anonymisées soit conservées pour une réutilisation ultérieure à des fins de recherche scientifique uniquement.

- 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 ;

- ***I/ <u>Le principe de sécurité</u>***

-

- 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.

-

-

- ***<u>J/ le principe de la confidentialité des données</u>***

- Aux termes de l’Article 385, << les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau >>

Merci pour votre aimable attention

Veuillez retrouver le présent slide : https://apdp.bj/formation-des-dpo-2021/

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/