RÉPUBLIQUE DU BÉNIN

AUTORITE DE PROTECTION DES DONNEES PERSONNELLES

GUIDE POUR LA MISE EN CONFORMITE AVEC LE REGIME DE PROTECTION DES DONNÉES PERSONNELLES AU BENIN

Ce guide pratique a été initié par l'Autorité de Protection des Données Personnelles (APDP) pour vous aider à comprendre le régime légal de protection des données personnelles et à vous mettre en conformité avec les prescriptions de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin telle que modifiée par la loi n° 2020-35 du 06 janvier 2021. Il ne décrit pas en détail toutes les prescriptions mais présente les démarches principales, les notions, les principes, les obligations et les sanctions.

I. NOTIONS PRINCIPALES

Pour bien comprendre ce guide, il faut garder à l'esprit les notions suivantes :

- **Données à caractère personnel :** toute information de quelque nature que ce soit et indépendamment de son support, relative à une personne physique identifiée ou identifiable ou susceptible de l'être directement ou indirectement, par référence à un ou plusieurs éléments spécifiques propre à son identité physique, physiologique, génétique, psychique, culturelle, social ou économique. Les nom, prénom, photographie, date de naissance, parenté, alliance, empreinte, adresse courriel, adresse postale, numéro de téléphone, matricule interne, immatriculation numéro de sécurité sociale, adresse IP, identifiant de connexion informatique, empreinte numérique, enregistrement vocal, numéro de carte bancaire, groupe sanguin, code ADN, etc...
- **Traitement :** toute opération ou tout ensemble d'opération portant sur des données quel que soit la finalité, la durée ou le procédé utilisé notamment la collecte, l'enregistrement, l'organisation, la consécration, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission ou diffusion de tout autre forme de mise à disposition.
- **Responsable de traitement :** Toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens.
- **Délégué à la protection des Données Personnelles DPDP (DPO) :** C'est la personne chargée de veiller à l'application du régime de protection des données personnelles dans l'organisme et de rendre compte à l'APDP envers laquelle il est tenu par un engagement.
- **Sous-traitant :** Toute personne physique ou morale, publique ou privée, qui traite des données pour le compte du responsable du traitement ou qui y aide. Le sous-traitant est soumis aux mêmes obligations incombant aux responsables de traitement.
- **Personnes concernées :** Toute personne physique dont les données à caractère personnel font l'objet d'un traitement.

II. LES PRINCIPES

Le traitement des données personnelles est régi par des principes. Le respect de ces principes vous permet de conformer vos activités à la loi. Peuvent être citées à ce titre de manière non exhaustive :

- **La licéité, la loyauté et la transparence :** Les données doivent être traitées de manière loyale, licite et transparente. La licéité du traitement s'entend de son fondement juridique (obligation légale, obligation contractuelle etc.).

  La loyauté du traitement désigne les modalités selon lesquelles les données sont collectées autant que les limites de l'habilitation du Responsable du traitement : le traitement sert une finalité et les données personnelles collectées ne pourront pas être réutilisées pour une autre finalité que celle qui a été habilitée.

  Cette habilitation doit avoir été obtenue de manière transparente. Le Responsable de traitement doit fournir à la personne concernée une information claire et intelligible sur le traitement. L'information concerne la nature du traitement, la finalité du traitement, le temps pendant lequel le Responsable du traitement utilise et conserve vos données, ceux à qui il les communique et l'exercice des droits à l'égard desdites données. Cette information doit être claire intelligible et mettre la personne concernée en mesure de décider en toute connaissance de cause.
  C'est une exigence de transparence et de bonne foi. L'obligation d'information concrétise en ce sens un droit opposable et garantit l'accès et l'opposition de la personne concernée.

- **La pertinence, la proportionnalité et le principe de minimisation :** Les données traitées doivent être pertinentes, adéquates et limitées au regard de la finalité poursuivie. Cela suppose que les données à caractère personnel qui ont été collectées sont bien en adéquation avec la finalité du traitement. La finalité correspond au but précis que le traitement doit atteindre. Seules les données qui sont adaptées à la finalité poursuivie c'est à dire ce à quoi doit servir le traitement envisagé, peuvent être traitées. La proportionnalité est le lien permanent entre collecte et finalité.

Le responsable de traitement ne doit pas collecter plus de données que ce dont il a vraiment besoin : c'est le principe de minimisation.

- **La limitation de la conservation des données :** il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une fois que l'objectif poursuivi par le traitement des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées ou anonymisées. La durée de conservation des données doit ainsi être limitée au strict minimum. Cette durée de conservation est définie par le Responsable de traitement ou la loi.
- **La sécurité des données personnelles :** Le responsable de traitement doit prendre toutes précautions utiles pour garantir la confidentialité et la sécurité des données qu'il traite. Il doit s'assurer que seules les personnes autorisées y accèdent, que les données restent intègres, complètes et ne sont l'objet d'aucun usage non autorisé. Les mesures à prendre à ce titre sont déterminées en fonction de divers paramètres (nature, sensibilité, intérêt, volatilité, valeur) et des risques pesant sur le traitement.

III. LES OBLIGATIONS

Les dispositions législatives prévoient diverses obligations à charge des responsables de traitement :

» Obligation de déclarer le traitement de données personnelles auprès de l'APDP (art. 405 , 407 CDN[1])

En quoi consiste-t-elle ?

Cette obligation met à la charge du responsable de traitement (organismes publics ou privés), la déclaration préalable auprès de l'Autorité de tous les traitements automatisés ou non automatisés (sauf les cas de dispenses prévus par les dispositions de l'article 410 du code du numérique) qu'il exécute et comportant des données à caractère personnel, avant leur mise en oeuvre ou, l'inscription dans un registre (Modèle de registre disponible à l'APDP ou sur son site via le lien: https://apdp.bj/les-outils-de-la-conformite/) tenu par la personne désignée à cet effet par ledit Responsable de traitement.

1 Code Du Numérique

Comment remplit-on cette obligation ?

Le Responsable de traitement devra :

- remplir le formulaire pour les formalités préalables ;
- se rapprocher de l'APDP muni de la liste de toutes les bases de données qu'il détient, des systemes d'informations ainsi que la liste exhaustive des éléments (catégories de données personnelles telles que nom et prénoms- situation matrimoniale...) qui composent chacune desdites bases de données, aux fins d'orientation vers le régime juridique de traitement approprié (régime déclaratif, autorisation).
- Dans certains cas il est demandé un avis préalable à l'Autorité par lettre adressée au Président de l'APDP. Cette demande d'avis décrit le traitement envisagé ou l'opération qui requiert l'avis avant sa mise en œuvre.

» Obligation d'information (art. 415 CDN)

En quoi consiste-t-elle ?

Elle consiste à communiquer à la personne concernée par le traitement, toutes les éléments d'appréciation tels que les informations relatives au responsable de traitement, la finalité dudit traitement, les droits, etc qui lui permettront de comprendre l'usage qui sera fait de ses données personnelles collectées et de donner librement et consciemment son accord/consentement.

Comment remplit-on cette obligation ?

Cette obligation est remplie par le responsable de traitement en mettant l'information (notamment celle indiquée par les dispositions de l'article 415 du code du numérique) à la portée de la personne concernée par divers moyens ou canaux de communication tels que les affiches, mentions sur formulaires, etc...

» Obligation d'assurer la confidentialité et la sécurité des données traitées (art.425-426 CDN)

En quoi consiste-t-elle ?

Elle consiste à traiter les données à caractère personnel de façon confidentielle et à mettre en place des mesures techniques et organisationnelles appropriées garantissant la sécurité des données.

Comment remplit-on cette obligation ?

Afin de garantir la sécurité des données à caractère personnel,

le Responsable de traitement et/ou le sous-traitant doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, l'interception notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

» Obligation de respecter des différents droits des personnes concernées par le traitement (art 415, 437, 440, 441, etc. CDN)

☑ En quoi consiste-t-elle ?

Le Responsable de traitement, le sous-traitant ou son représentant doit garantir aux personnes dont les informations sont traitées, une série de droit défini par le législateur : le consentement, le droit à l'information préalable, le droit d'accès, le droit d'opposition, le droit de rectification et de suppression, le droit à l'oubli, etc

☑ Comment remplit-on cette obligation ?

Ces droits sont assurés par le Responsable de traitement lorsqu'il indique aux personnes concernées les modalités d'exercice des différents droits. La mise en place au sein de la structure d'un service de réclamation ou de gestion de ce type de requête est également recommandée.

» Obligation de tenir un registre des activités liées au traitement (art. 435 CDN)

☑ En quoi consiste-t-elle ?

Chaque Responsable du traitement et, le cas échéant, le représentant du responsable du traitement tient un registre des activités de traitement effectuées sous sa responsabilité. Ce registre comporte des mentions obligatoires définies par le législateur.

☑ Comment remplit-on cette obligation ?

Cette obligation est remplie par le Responsable de traitement lorsqu'il tient et met à jour un registre physique de toutes les activités de traitement effectuées dans sa structure.

Un modèle de registre des activités de traitement est disponible auprès de l'Autorité. (https://apdp.bj/wp-content/uploads/2021/11/Registre-des-activites-de-traitement.xls

» **Obligation d'établir un rapport annuel à transmettre à l'APDP (art. 387 CDN).**

☑ **En quoi consiste-t-elle ?**

Le responsable de traitement ou son représentant est tenu d'établir tous les ans, un rapport annuel des activités de traitement qu'il a menées. Il adresse ce rapport à l'APDP au plus tard le 30 juin de l'année suivant celle de l'activité.

☑ **Comment remplit-on cette obligation ?**

Le rapport annuel d'activité à produire porte d'une part, sur toute diligence effectuée pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 383, 389, 395, 396 et 397 du code du numérique puis d'autre part, sur l'accès restreint aux données traitées par les personnes habilités.

IV. LES 10 POINTS DE LA CONFORMITÉ

L'APDP vous propose une démarche de mise en conformité en dix points. Les étapes ne sont pas nécessairement successives.

1. Evaluer et identifier toutes les opérations de traitement[2] de données que vous effectuez dans votre administration ou entreprise (structure). Cela signifie :

Cela signifie :

a. répertorier les données personnelles qui sont collectées ou utilisées (Nom, prénom, date de naissance, photo ou copie de pièces d'identité, groupe sanguin, curriculum vitae, numéro de téléphone, autres numéros personnels, religion, ethnie,...) ;

2 Les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires et peuvent être autorisés par une décision unique de l'Autorité. Dans ce cas, le responsable de chaque traitement adresse à l'Autorité un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

b. définir les finalités de tous traitements de ces données (gestion de paie, ..) ;

c. classer et distinguer les opérations et les données par finalité ;

d. identifier et désigner le(s) responsable(s) de traitement[3] ;

e. Constituer le registre de traitement de votre structure.
(https://apdp.bj/les-outils-de-la-conformite/)

Vous avez fait le plus dur !

2. Déterminer et identifier les intervenants et prestataires susceptibles d'avoir accès aux systèmes, données et traitements.

Cela signifie :

a. dentifier les personnes, les prestataires ou partenaires qui traitent des données personnelles pour le compte de votre administration ou entreprise (expert-comptable, gestionnaire de paie, gestionnaire du coffre- fort numérique, hébergeur, prestataire de maintenance informatique, société de sécurité, développeur d'applications ou de logiciels...). Il pourrait s'agir des agents, les fournisseurs, les sous-traitants ;

b. les informer par écrit (mail ou courrier) de leurs obligations et mettre en place leurs engagements juridiques en termes de confidentialité, respect des finalités, sécurité. (annexe au contrat de travail, etc..).

Voilà aussi une bonne chose de faite !

3. Concevoir et mettre en place les mesures de sécurité

a. choisir les équipements et matériels adéquats

b. penser et mettre en place la sécurité environnementale des systèmes d'informations, des données et des traitements

c. prendre conseil pour les mesures de sécurité logicielle

3 Le code du numérique a mis à la charge du responsable du traitement plusieurs obligations. Ainsi, un responsable de traitement qui manipule les données personnelles quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement) fait une opération/traitement et est soumis à certaines obligations en vigueur en matière de protection desdites données.

d. adopter la politique interne de sécurité PSSI (politique de confidentialité, note interne, charte d'utilisation des outils informatiques, niveaux de classification des documents et mails, gérer les accès et les habilitations.).

Prenez des conseils !

4. Saisir l'Autorité de Protection des Données à caractère Personnel pour les formalités préalables[4]

a. visiter le site internet de l'APDP (**https://apdp.bj/procedures/**) pour formaliser une demande, ou prendre rendez-vous

b. fournir toutes les pièces justificatives.

C'est gratuit mais obligatoire[5] !

5. Sensibiliser les collaborateurs et agents aux problématiques et enjeux de la protection des données personnelles.

a. cette sensibilisation peut être faite par tous moyens (en présentiel, par la diffusion d'une note d'information, l'actualisation du règlement intérieur, la signature d'un engagement de confidentialité...) ;

4 La demande est présentée par le responsable du traitement. L'autorisation n'exonère pas de la responsabilité à l'égard des tiers.

5 Les formalités préalables (déclaration de traitement des données ou demande d'autorisation selon le cas), sont prévues par les articles 405 et 407 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, telle que modifiée par la loi n° 2020-35 du 06 janvier 2021.

b. mettre en œuvre les outils nécessaires au respect des principes et obligations du régime de protection des données personnelles (prévoir des mentions d'information dans les mails, dans les CGU/CGV, dans les courriers, sur des formulaires de collecte… ; le cas échéant, informer oralement les interlocuteurs par téléphone.).

L'adhésion est nécessaire à la réussite !

6. Informer les personnes concernées de l'existence d'un traitement de leurs données personnelles et demander leur consentement.

L'APDP met à votre disposition des outils pour vous aider

https://apdp.bj/wp-content/uploads/2021/11/Consentement_de_collecte.pdf

Vous respectez la loi !

7. Désignation d'un Délégué à la Protection des Données Personnelles (DPDP ou Data Protection Officer) en charge des problématiques de protection des données personnelles.

La désignation du Délégué à la Protection des Données Personnelles est rendue publique et notifiée à l'APDP avec lequel il prend un engagement

(https://apdp.bj/wp-content/uploads/2022/01/Lettre.Engagement.DPO_-valide_OK.pdf)

Votre conscience au quotidien !

8. Respecter les droits des personnes concernées d'accéder aux données les concernant, de s'opposer à un traitement, de demander l'effacement de leurs données.

Cela implique :

a. de mettre en place un processus de gestion des réclamations des personnes concernées pour leurs données personnelles ;

b. mettre en place un processus de notification des violations de données personnelles (incidents de sécurité ayant impacté les données personnelles, accès non autorisé, fuite volontaire ou accidentelle de données, indisponibilité involontaire ou anormale des données, suppression ou modification intentionnelle ou accidentelle des données...).

C'est l'un des objectifs !

9. Assurer en permanence la sécurité des traitements :

Il s'agit :

a. d'appliquer en intégralité les directives du régime de protection des données personnelles ;

b. de veiller à tout le moins à respecter les mesures élémentaires préconisées, à savoir :

» Sécuriser les fichiers :

- ☑ sécuriser l'accès au fichier (gestion des droits d'accès) ;
- ☑ mettre un mot de passe à l'ouverture du fichier s'il contient des données sensibles (données de santé ou numéro de sécurité sociale par exemple) ;
- ☑ mise en place de logs pour être en mesure de détecter les intrusions en cas de vol de fichiers, d'accès non autorisé, de fuite de données..;
- ☑ avoir une sauvegarde du fichier ou de ses données pour être en mesure de restaurer un fichier modifié ou supprimé.

» Sécuriser les équipements :

- ☑ mettre un mot de passe individuel un code de verrouillage de l'appareil ou Crypter l'ordinateur ou la tablette ;
- ☑ Utiliser un MDM (Mobile Device Management) qui permet de gérer les tablettes ou smartphones à distance afin d'effacer les données en cas de perte / vol du terminal ;
- ☑ avoir un antivirus à jour ;
- ☑ mettre régulièrement à jour le système d'exploitation, les outils, logiciels ou applications utilisés.

» Réaliser régulièrement des audits des systèmes d'information et de l'infrastructure technique

b. veiller à la conservation des données

C'est l'effort constant !

10. Présenter les rapports périodiques et se faire délivrer le certificat de conformité de l'APDP.

APDP

AUTORITE DE PROTECTION DES DONNEES PERSONNELLES

POUR PLUS D'INFORMATION SUR LE SUJET, VEUILLEZ :

- VISITER LE SITE INTERNET DE L'APDP À L'ADRESSE : **https://www.apdp.bj**
- CONTACTER L'APDP :
  - AU TÉLÉPHONE : (+229) 21 32 57 88
  - PAR EMAIL : contact@apdp.bj
- VOUS RENDRE AU SIÈGE DE L'APDP : Rue 6.076 (Centre d'accueil monseigneur Parisot) Aïdjèdo, Immeuble El MARZOUK Joël.

@apdp.benin (+229) 69 55 00 00 @APDP_BENIN