RÉPUBLIQUE DU BENIN

Rue 6.076 « Aïdjèdo, Immeuble El MARZOUK Joël »
01 BP : 04837 Cotonou
+229 21 32 57 88 / 69 55 00 00
contact@apdp.bj
IFU : 4201810471821
www.apdp.bj

FICHE PRATIQUE

POUR LA MISE EN CONFORMITE DES OBLIGATIONS RELATIVES A LA PROTECTION DES DONNÉES PERSONNELLES

Cette fiche pratique a été initiée par l'Autorité afin de vous aider à comprendre le régime légal de protection des données personnelles et à vous mettre en conformité avec les prescriptions de 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. Elle ne décrit pas en détail toutes les prescriptions mais présente les éléments clés, les textes applicables, les principes ainsi que les sanctions.

I. QUELQUES NOTIONS

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. Il s'agit de toute information relative à une personne physique identifiable ou susceptible de l'être, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. L'identification se fait à partir des moyens dont dispose ou auquel peut avoir accès, le responsable du traitement ou toute autre personne.

Traitement : Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, le cryptage, l'effacement ou la destruction

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.

Sous-traitant : Toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement. Le sous-traitant est soumis aux mêmes obligations incombant aux responsables de traitement.

Personnes concernées par un traitement de données à caractère personnel : Toute personne physique dont les données à caractère personnel font l'objet d'un traitement.

II. QUE FAIRE ? Les 10 points de la conformité

1. Evaluer et identifier toutes les opérations de traitement[1] de données que vous effectuez dans votre administration ou entreprise (structure). 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,…) ;
- **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 ; [2]
- **e.** Constituer le registre de traitement de votre structure.

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.** identifier 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..).

[1] 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.

[2] 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.

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 ;
- **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 [3]

- **a.** visiter le site internet de l'APDP (www.apdp.bj) pour formaliser une demande, prendre rendez-vous ;

- **b.** fournir toutes les pièces justificatives.

C'est gratuit mais obligatoire[4] !

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...) ;

- **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.

Vous respectez la loi !

---

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

[4] : 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.

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.**

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 :**
   a. *appliquer en intégralité les directives du régime de protection des données personnelles ;*
   b. *veiller à tout le moins à respecter les mesures élémentaires préconisées*

- ***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) ;*

  - m*ise 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***

c. *veiller à la conservation des données*

L'effort constant !

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

III. LES FORMALITÉS ET REGIMES

Tout responsable de traitement qui soumet sa requête de déclaration, autorisation ou plainte à l'APDP, devra au préalable remplir un formulaire selon le type de traitement envisagé. Il s'agit de :

- **Avis :** lettre officielle adressée au Président de l'Autorité. Ce document devra décrire de manière claire et précise le traitement ou l'opération qui requiert l'avis de l'Autorité avant sa mise en œuvre ;
- **le formulaire de demande d'autorisation :** à remplir lorsque le traitement envisagé requiert une autorisation ;
- **le formulaire de déclaration (3 différents types de formulaires de déclarations sont disponibles)** : à remplir lorsque le traitement envisagé nécessite une déclaration auprès de l'Autorité ;
- **la fiche de plainte / le formulaire de signalement** : à renseigner en cas de plainte ;

IV. LES PRINCIPES ET OBLIGATIONS

- **Obligation de déclarer le traitement de données personnelles auprès de l'APDP (art. 405 ; 407) ;**
    - **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)** tenu par la personne désignée à cet effet par ledit responsable du traitement.

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

Le responsable de traitement devra se rapprocher de l'Autorité munit 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).

- **Obligation de respecter les différents principes de protection des données personnelles (art.383-384-385-387- 389-390) ;**

    - **En quoi consiste-t-elle ?**

Le responsable de traitement doit respecter les principes cardinaux de la protection des données personnelles telles que: les principes de consentement et de légitimité, de licéité et de loyauté du traitement des données à caractère personnel, de la finalité, de la proportionnalité, de la conservation limitée des données personnelles, du respect des droits des personnes concernées, de confidentialité et de sécurité…

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

Le Responsable de traitement, le sous-traitant ou le Délégué à la protection des données personnelles doit y veiller en faisant un suivi de l'activité exercée par les personnes habilitées les bases de données et contrôler de façon régulière et systèmatique l'usage qui en est fait.

- **Obligation d'information (art. 415) ;**

    - **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) ;**

    - **En quoi consiste-t-elle ?**

Elle consiste à traiter les données à caractère personnel de façon confidentielle et de 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 du traitement et/ou son sous-traitant doivent 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.

Il incombe également au responsable du traitement, son représentant ainsi qu'au sous- traitant de veiller au respect de ces mesures de sécurité.

- **Obligation de respecter des différents droits des personnes concernées par le traitement (art 415/437/440/441…)**

    - **En quoi consiste-t-elle ?**

Le responsable de traitement, son sous-traitant ou son représentant doit garantir aux personnes dont les informations sont traitées, une série de droit définie 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) ;**

    - **En quoi consiste-t-elle ?**

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. 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.

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

    - **En quoi consiste-t-elle ?**

Le responsable de traitement ou son représentant est tenu d'établir tous les ans, un rapport annuel pour le compte de l'Autorité.

- **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.

V. LES ACTEURS

- **Le Responsable du traitement ou son représentant ou le sous-traitant ;**
- **Le Délégué à la protection des données personnelles :** Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

  Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère les dispositions du livre V^{ème} du code du numérique.

VI. DROITS DES PERSONNES CONCERNEES

La loi reconnait des droits aux personnes dont les données sont traitées. Le responsable de traitement doit garantir les droits des personnes concernées.

- **Droit à l'information préalable (art. 415) ;**

  - **En quoi consiste-t-il ?**

Elle consiste à communiquer aux personnes concernées par le traitement, certaines informations obligatoires définies par le législateur à travers les dispositions de l'article 415 du code du numérique.

  - **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en mettant les informations prédéfinies à la disposition des personnes concernées aux moyens de canaux de communication appropriés (affiches, information via courriel/site web, etc).

- **Droit d’accès (art. 437) ;**

    - **En quoi consiste-t-il ?**

La personne dont les données sont collectées et traitées peut demander au responsable de ce traitement de lui communiquer certaines informations la concernant. La liste des requêtes auxquelles le responsables de traitement doit accéder est prevue aux dispositions de l’article 437 du code du numérique.

    - **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en indiquant aux personnes concernées, les modalités d’exercice (requête écrite, formulaire de réclamation à renseigner, courrier électronique ou postal…) dudit droit et en répondant dans le délai légal prévu par le législateur.

- **Droit d’opposition (art. 440) ;**

    - **En quoi consiste-t-il ?**

C’est le droit reconnu à toute personne physique 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.

    - **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en indiquant aux personnes concernées, les modalités d’exercice (requête écrite, formulaire de réclamation à renseigner, courrier électronique ou postal…) dudit droit et en répondant dans le délai légal prévu par le législateur.

- **Droit de rectification et de suppression (art. 441) ;**

    - **En quoi consiste-t-il ?**

Toute personne physique peut exiger du responsable du traitement que soient, selon les cas, et dans les meilleurs délais, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, non pertinentes ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

    - **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en indiquant aux personnes concernées, les modalités d’exercice (requête écrite, formulaire de réclamation à renseigner, courrier électronique ou postal…) dudit droit et en répondant dans le délai légal prévu par le législateur.

- **Droit à l'oubli (art. 443);**

    - **En quoi consiste-t-il ?**

Elle est l'obligation pour un moteur de recherche / responsable de traitement, de supprimer de la liste de résultats affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne .

    - **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en indiquant aux personnes concernées, les modalités d'exercice (requête écrite, formulaire de réclamation à renseigner, courrier électronique ou postal…) dudit droit.

- **Droit à la portabilité des données (art. 438) ;**

    - **En quoi consiste-t-il ?**

C'est le droit d'une personne concernée de recevoir les données à caractère personnel la concernant qu'elle a fournie a un responsable du traitement, dans un format structuré, couramment utilisable et lisible par machine, et a le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle ceci, dans les conditions prévues par les dispositions de l'article 438 du code du numérique.

    - **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en indiquant aux personnes concernées, les modalités d'exercice (requête écrite, formulaire de réclamation à renseigner, courrier électronique ou postal…) dudit droit.

- **Droit d'interrogation (art. 439) ;**

    - **En quoi consiste-t-il ?**

Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en oeuvre les traitements automatisés dont la liste est accessible au public en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication.

- **Comment remplit-on ce droit ?**

Le responsable de traitement garantit ce droit en indiquant aux personnes concernées, les modalités d'exercice (requête écrite, formulaire de réclamation à renseigner, courrier électronique ou postal…) dudit droit.

- **Droit à réparation et responsabilité (art. 451).**

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation des dispositions du livre V^{ème} sur la protection des données à caractère personnel a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation des dispositions du Livre V^{ème}. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par les dispositions du livre V^{ème} qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.