REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Par Ambroise Dj. ZINSOU
Consultant Télécoms et Protection
des données personnelles
et de la vie privé

Novembre 2021

SOMMAIRE

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

1 CONTEXTE

Développement sans précédent des TIC ;

Globalisation de l'économie numérique;

Multiplication des possibilités de collecte et la capacité de traitement des données des systèmes, (les Big Data);

Explosion des réseaux sociaux, l'augmentation de la puissance et de l'efficacité des moteurs de recherche, les moyens de géolocalisation et vidéosurveillance, l'arrivée de la biométrie…;

Accroissement des risques d'atteinte aux libertés publiques et à la vie privée.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Mise en place d'une législation de protection des données à caractère personnel qui permettent de sauvegarder les libertés individuelles en sorte que les TIC **« ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »** (**Article 379 alinéa 3 du code du numérique**)

2. **Définitions**

Au sens du code du numérique on entend par :

i) **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.

2. Définitions

ii. Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des 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).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

3. IMPORTANCE DU TRAITEMENT DES DONNEES PERSONNELLES

- Les données à caractère personnel collectées par les organismes publics et privés sont au cœur des évolutions des rapports entre les organisations et leurs usagers ;

- A l'ère de la « **globalisation de la surveillance** » policière et du marketing, les technologies de l'information et de la communication ont contribué largement à généraliser, dans tous les secteurs, des pratiques de prélèvement systématique, d'exploitation des données privées et des traces des individus pour des raisons de sécurité des Etats à l'heure de la guerre contre le terroriste et de la « globalisation de l'économie ».

- Les pratiques de collecte, de conservation et d'exploitation d'informations relatives à des individus font partie des modes d'administration des populations .

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

4. LES REGIMES DE TRAITEMENT DES DONNEES PERSONNELLES

4.1. Elaboration de la politique de classification des données

- La classification des données est la composante essentielle de tout programme de sécurité et de conformité de l'information, en particulier si l'organisation traite un volume important d'information;

- Difficulté pour l'organisation de maintenir un contrôle sur sa base de données si elle ne sait, ni ne maitrise ou ignore le lieu de son hébergement pour assurer le plus haut niveau de protection surtout si lesdites données ne sont pas classifiées en fonction de leurs niveaux de sensibilité et de leur valeur.

- La première étape consiste à élaborer **une politique de classification** des données afin de définir quelles sont les données sensibles, et d'établir des règles pour leur protection.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

4.2. Politique de classification des données

Il s'agit d'un document qui comprend un *cadre* de classification, *une liste des responsabilités pour identifier les données sensibles* et la description des différents niveaux de classification des données, l'objectif étant de protéger les données contre des risques tels que leur divulgation et accès non autorisés.

NB: **La politique de classification de l'information ne doit pas inclure d'exigences sur la façon dont les données doivent être traitées. Il faut plutôt élaborer un document distinct qui définit les exigences relatives à la protection de chaque classe de données.**

Les politiques peuvent différer dans leurs objectifs et leur structure globale, mais une bonne norme de classification des données répondra aux critères suivants :

- Simples pour éviter toute ambiguïté, mais suffisamment génériques pour s'appliquer à différents actifs dans différents contextes ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Claire et rédigée dans un langage simple ;
- Adapter aux activités de l'organisation ;
- Comporter que quelques pages, et n'avoir pas plus de trois ou quatre niveaux de classification ;
- Contenir un point de contact pour tous les cas extrêmes et les situations auxquelles les employés peuvent être confrontés;
- Contenir un calendrier de révision.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

4.3. Etapes pour l'élaboration d'une politique de classification des Données personnelles.

Sept (07) étapes suivantes devront être suivies :

i. Étape 1. **Sollicitez l'aide de cadres d'un niveau supérieur**

- Recourir au démarrage à l'appui d'une personne de haut niveau dans l'organisation qui comprend l'importance de la classification et les risques associés aux données.

- Associer toutes les parties prenantes pour les prochaines étapes.

ii. **Étape 2 : Définir le but de la classification des données sensibles.**

Expliquer aux parties prenantes l'importance de la mise en oeuvre d'une politique de classification des données.

Pour mener à bien l'élaboration de la politique, les démarches suivantes devront être suivies :

- Cartographier les niveaux de protection des données en fonction des besoins, des budgets et des contraintes de ressources de l'organisation ;
- Atténuer les risques associés à la divulgation et aux accès non autorisés;
- Être en conformité avec les normes qui exigent la classification de l'information (**p. ex., ISO 27001**), la récupération d'informations spécifiques dans un délai déterminé ou le stockage des données dans des endroits spécifiques avec un accès limité

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

iii. Étape 3. Définir la portée de la politique.

- Définir la portée de la politique en fonction de la quantité d'informations à traiter avant de procéder à la classification en fonction du niveau de sensibilité des données;
- Présenter les données sous différentes formes, et les stocker sur différents supports (physiques, mémoire de masse, USB et des cartes mémoire,.. etc…)

iv. **Étape 4. Préciser les responsabilités.**

- Déterminer qui sera responsable de la mise à jour des protocoles de classification des données pour chaque élément de données. (rôles des propriétaires, des gestionnaires et utilisateurs de données, ainsi que les employés, le personnel de la direction, du service juridique, de la gestion des dossiers et du service de conformité.)

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

iv. Étape 5. Définir les niveaux de sensibilité des données.

- Préciser les niveaux de classification et les sources de données, les définitions;

- Donner des exemples pour chaque niveau. Il n'y a pas de norme stricte pour un tableau de classification des données. Il doit être développer en fonction de la complexité de l' environnement informatique, de l'organisation, des exigences de la structure. Cependant, il est fortement recommandé de maintenir le nombre de niveaux de classification des données à au plus 4 niveaux, car il est extrêmement difficile de mettre en pratique un schéma plus complexe. En général, ces niveaux sont similaires aux suivants :

  - Niveau 1 : Données très sensibles de l'entreprise ou des clients ;
  - Niveau 2 : Données internes sensibles ;
  - Niveau 3 : Données internes qui ne sont pas destinées à être divulguées au public ;
  - Niveau 4 : Données pouvant être divulguées au public.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

vi. Étape 6. Élaborer des lignes directrices pour assurer la sécurité des données.

Elaborer un ensemble d'activités et de règles sur la protection des données en rapport avec son niveau de criticité.

NB: le tableau de traitement des données doit être différent de la politique de classification des données u fait du caractère mouvant de l'environnement sécuritaire;

vii. Étape 7. Réviser et affiner.

La politique de classification des données et les directives de traitement des données doivent être revisitées périodiquement pour y apporter des modifications si nécessaire.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

4.4. Exemples de classification des données dans les secteurs public et commercial

S'inspirer des modèles réussis, d'entités de renommées des secteurs public et privé, comme guides

i) *Exemple 1 : Niveaux de classification des données gouvernementales*

Le système typique de classification des données gouvernementales utilisé par les gouvernements fédéraux, étatiques et locaux n'assigne pas plus de trois niveaux de sensibilité : top secret, secret et données publiques.

ii. *Exemple 2 : Niveaux de classifications des données commerciales*

4 niveaux de classification des données sont utilisés, dont trois niveaux confidentiels (secret, confidentiel, utilisation commerciale seulement et un niveau public.

4.5. Classification des données personnelles

Organiser les données par catégories selon des critères convenus pour permettre l'utilisation plus efficace des données critiques et leur protection dans l'ensemble de l'entreprise. La classification des données participe également à la gestion des risques et des processus de connaissances légales et de conformité.

La classification des données aide à améliorer la sécurité des données et le respect de la réglementation (**La sécurité des données critiques, Conformité avec les obligations réglementaires**)

4.6. Lignes directrices pour la classification des données

le processus de classification peut être décomposé en quatre étapes clés, qu'on peut personnaliser pour répondre aux besoins spécifiques de l'organisation lorsqu'on développe la stratégie de protection des données.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

i. Étape 1. Mettre en place une politique de classification des données.

- Définir une politique de classification des données et la communiquer à tous les employés.. La politique doit être courte, simple et inclure les éléments de base suivants :

  - **Les objectifs** : Les raisons pour lesquelles la classification de données a été mise en place et les attentes de l'organisation ;
  - **Le flux de travail** : Comment le processus de classification de données sera organisé et quel sera l'impact sur les employés qui exploitent les différentes catégories de données sensibles ;
  - **Le schéma de classification de données** : Les catégories de classement des données ;
  - **Les propriétaires de données** : Les rôles et responsabilités des unités de traitement y compris la manière de classer les données sensibles et d'en octroyer l'accès;
  - **Les instructions de manipulations** (Les normes de sécurité , les habilitations, les processus et les termes de sauvegarde, etc)

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

ii. Étape 2. Identifier les données sensibles.

- Procéder à la cartographie des données une fois la politique établie.
- Automatiser l'identification des données à l'aide d'applications conçues pour déterminer les systèmes et les ressources, comme les bases de données ou les partages de fichiers, qui peuvent contenir des informations sensibles.

iii. Étape 3. Mettre en place des étiquettes.

- Attribuer une étiquette à chaque ressource de données sensibles pour améliorer la mise en œuvre de la politique de classification données. L'étiquetage peut être automatisée selon le schéma de classification des données ou effectué manuellement par les propriétaires des données.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

iv. Étape 4. Utiliser les résultats pour améliorer la sécurité et la conformité.

Passer en revue les stratégies de sécurité une fois que l'emplacement de chaque catégorie de données sensibles est connu pour évaluer si toutes les données sont protégées par des mesures appropriées par rapport aux risques encourus.

v. Étape 5. Répéter les étapes.

Les données ne sont pas figées, elles évoluent de façon dynamique. En effet, chaque jour, des fichiers sont créés, copiés, déplacés et supprimés. Par conséquent, la classification des données doit être un processus continuel au niveau de l'organisation.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Exemples de catégories de classification données

Il n'y a pas une façon unique de concevoir un modèle de classification des données. Une des options consiste à commencer avec un type simple de classification des données sur trois niveaux :

- **Les données publiques** qui peuvent être librement divulgués dans le public (p. ex., les contacts de service clients) ;
- **Données internes** dont les exigences de sécurité sont faibles et ne sont pas destinées à être divulguées au public ;
- **Données restreintes** – sont des données très sensibles dont la divulgation pourrait affecter négativement les opérations et mettre l'organisation en danger financier ou juridique (p. ex., les données personnelles des clients, patients et employés, les données d'authentification tels que les identifiants de connexion et les mots de passe).

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

5. Données personnelles sensibles

5.1. Définition

Le code du numérique définit les Données sensibles comme 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 ;

5.2. Données sensibles et exceptions [Art 394 CDN]

Le code du numérique interdit de recueillir ou d'exploiter les d**onnées sensibles** sauf, notamment, dans les cas suivants :

- Les informations sont manifestement rendues publiques par la personne concernée ;
- La personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée). Le consentement peut être retiré à tout moment sans frais par la personne concernée ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Le traitement des données personnelles de la personne concernée est nécessaire à la sauvegarde de ses intérêts vitaux ou ceux d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- L' utilisation des données personnelles est justifiée par l'intérêt public et autorisée ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une Autorité publique ou est assigné par une Autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;
- Le traitement est effectué en exécution de lois relatives à la statistique publique ;
- Le traitement est nécessaire aux fins de médecine préventive ou la médecine du travail, de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et le traitement est effectué sous la surveillance d'un professionnel des soins de santé ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tel que la protection contre les menaces transfrontalières graves pesant sur la santé, aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux sur la base du droit en vigueur, qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;
- Le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu des dispositions du présent Livre, en vue de l'application de la sécurité sociale ;
- 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 la personne concernée pendant la période précontractuelle;
- Le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;
- Le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Le traitement est effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par l'Autorité et que les données ne soient pas communiquées à des tiers sans le consentement écrit des personnes concernées, que ce soit sur un support papier, support électronique ou tout autre support équivalent ;

- Le traitement est effectué dans le cadre des activités légitimes et moyennant les garanties appropriées d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter exclusivement aux membres ou anciens membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à ses objectifs et à sa finalité, et que les données ne soient pas communiquées à un tiers extérieur sans le consentement des personnes concernées ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Le traitement est nécessaire 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.

Ainsi donc, en cas de traitement des données sensibles ou des données concernant des personnes vulnérables, il faut prendre des mesures complémentaires

6. ANONYMISATION [Articles 33 et 34 CDN]

6.1. Définition

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification d'une personne par quelque moyen que ce soit et de manière irréversible.

6.2. Critères d'anonymisation

En France par exemple, La Commission Nationale Informatique et Libertés (CNIL) a défini trois grands critères à respecter pour qu'une donnée soit officiellement considérée comme anonyme :

- la corrélation ;
- l'inférence ;
- l'individualisation.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

i. Corrélation

Ce critère consiste à ne pas conserver deux données concernant la même personne dans une ou plusieurs bases de données l'entreprise ou de l'organisation.

Par exemple : les numéros de téléphone des clients se retrouve dans plusieurs bases de données.

ii. Inférence

L'inférence revient à tirer une conclusion à partir d'un fait ou d'une situation déjà vérifiées.

Par exemple, la base de données d'une entreprise contient des informations sur le statut de ses clients dans laquelle toutes les femmes de 35 à 40 ans sont mariées. Dans ce cas, il sera très facile de déduire que Madame X âgée de 36 ans est mariée.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

iii. Individualisation

La question à se poser : est-il toujours possible d'isoler une personne ?

L'individualisation revient à différencier une personne par des caractères individuels qui lui sont propres. Pour respecter ce critère, **les données détenues par une organisation ne doivent pas permettre d'isoler une personne et donc de l'identifier.**

Par exemple lorsqu'une entreprise remplace les noms et prénoms de ses clients par des numéros. Cette action revient alors à les individualiser

La technique d'anonymisation appliquée n'est pas efficace si l'un de ces trois critères n'est pas respecté.

6.3. Méthode d'anonymisation

Pour construire un processus d'anonymisation pertinent, il faut :

- Identifier les informations à conserver selon leur pertinence ;
- Supprimer les éléments d'identification directes ainsi que les valeurs rares qui pourraient permettre une ré-identification aisée des personnes (par exemple, la présence de l'âge des individus peut permettre de ré-identifier très facilement les personnes centenaires) ;
- Distinguer les informations importantes des informations secondaires ou inutiles (c'est-à-dire supprimables) ;
- Définir la finesse idéale et acceptable pour chaque information conservée.

Ce prérequis permet de déterminer le procédé d'anonymisation à appliquer

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Celles-ci peuvent être regroupées en deux familles : **la randomisation et la généralisation.**

i) La **randomisation** consiste à modifier les attributs dans un jeu de données de telle sorte qu'elles soient moins précises, tout en conservant la répartition globale. Cette technique permet de protéger le jeu de données du risque *d'*inférence .

- **Exemple : il est possible de permuter les données relatives à la date de naissance des individus de manière à altérer la véracité des informations contenues dans une base de données.**

ii. La **généralisation** consiste à modifier l'échelle des attributs des jeux de données, ou leur ordre de grandeur, afin de s'assurer qu'ils soient communs à un ensemble de personnes. Cette technique permet d'éviter l'individualisation d'un jeu de données. Elle limite également les possibles corrélations du jeu de données avec d'autres .

6.4. Protection contre les risques liés à l'anonymisation

À défaut de remplir parfaitement ces trois critères, le responsable de traitement qui souhaite anonymiser un jeu de données doit démontrer, via une évaluation approfondie des risques d'identification, que le risque de ré-identification avec des moyens raisonnables est nul.

Les techniques d'anonymisation et de ré-identification étant amenées à évoluer régulièrement, il est indispensable pour tout responsable de traitement, d'effectuer une veille régulière pour préserver, dans le temps, le caractère anonyme des données produites..

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

7. Pseudonymisation

La pseudonymisation est une alternative à l'anonymisation.[processus irréversible]

Le code du numérique la définit comme un « **traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable** » [Art. 424 et 426 CDN]

C'est un traitement qui consiste à remplacer les attributs identifiables d'une personne par une clé d'identification telle qu'un numéro par exemple. Cette méthode permet donc de sécuriser les données personnelles de manière réversible. Les utilisateurs peuvent exploiter les jeux de données sans pour autant réussir à identifier les personnes. La clé d'identification leur permet de ré identifier les données à tout moment.

Le point critique de la pseudonymisation est sa clé d'identification permettant de rétablir le lien entre les données pseudonymisées et l'identité des individus concernés.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

8. LES REGIMES DE TRAITEMENT

Au Bénin, quatre (04) régimes sont appliqués :

- le régime d'autorisation ;
- le régime de déclaration ;
- les avis ;
- les plaintes et pétitions.

Avant la mise en œuvre d'un traitement, le responsable de traitement est astreint à remplir des formalités préalables en fonction des types de données à traiter auprès de l'Autorité de Protection des Données Personnelle [APDP].

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Ainsi, la loi a établi une distinction dans les régimes en fonction de la nature des données par rapport aux risques que représente le traitement à l'égard du droit des personnes.

Tandis que les traitements de données **non sensibles** sont soumis à un régime de déclaration, les traitements de **données sensibles** sont soumis à un régime d'autorisation auprès de l'Autorité de contrôle

i) **Le régime de déclaration [Article 405 du CDN]**

Pour les données non sensibles, une simple déclaration de conformité aux normes simplifiées élaborées est exigée. Il s'agit des traitements qui ne sont pas susceptibles de *porter atteinte aux droits et libertés des personnes concernées. Toutefois il y a une* dispense de déclaration à l'autorité à savoir qu'au lieu d'une déclaration, le responsable de traitement peut inscrire les traitement « **dans un registre tenu par la personne désignée à cet effet par le responsable du traitement»**. L'intérêt de l'introduction de ce dispositif est de limiter les fichiers clandestins puisque la tenue du registre pourrait conduire à **« révéler »** à l'autorité les fichiers non déclarés. Au nombre des traitements de déclaration simple, on peut citer les déclarations des systèmes de vidéosurveillances, des sites WEB et autres traitements de données non sensibles.

Un récépissé est délivré aux demandeurs par l'APDP à l'issue de l'étude du dossier.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Formulaire de déclaration simple

FORMULAIRE
APDP_DECLARATION

ii. **le régime d'autorisation** [**Article 394 du CDN**]

Lorsque le traitement concerne des données à caractère personnel sensibles [Article 394 duCDN], celui-ci est soumis à un régime d'autorisation. Sont considérées comme données sensibles les traitements ci-après :

- traitements de données personnelles **« révélant l'origine raciale ou ethnique, les opinions politiques, Le traitement de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique »**

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Conformément aux dispositions de l'article 428 du CDN, les traitements énumérés ci-dessus et réputées sensibles doivent faire l'objet d'une analyse d'impact en cas de risque élevé pour les droits et libertés des personnes concernées par le traitement et surtout s'il s'agit d'un « **traitement à grande échelle de catégories particulières de données visées à l'article 394, alinéa premier, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395** »

Toutefois, pour certains types de traitements en raison de la sensibilité particulière des données traitées, des articles spécifiques du code autorisent des régimes dérogatoires [**Article 394 et 407 du CDN**] pouvant inclure des formalités, au titre de garanties ou de conditions supplémentaires.[Article 394 et 407 point 1 à 5 du CDN]

Il en va ainsi pour les traitements [Article 407 points 1 à 8]:

- des données visées aux articles 394 et 397 du CDN ;
- D'un numéro d'identification national ou de tout autre identifiant d'application générale ;
- Des données génétiques, biométriques ou des données concernant la santé Article 407 points 1 à 8 du CDN;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Des données à caractère personnel ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques ;
- Des données à caractère personnel ayant pour objet une interconnexion de fichiers ;
- Liés au transfert de données à caractère personnel envisagé à destination d'un État tiers ;
- automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;
- automatisés de données comportant des appréciations sur les difficultés sociales des personnes;
- Des données à caractère personnel mis en œuvre pour le compte des services publics de l'Etat [article 411 du CDN] et qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Des données à caractère personnel relatives aux condamnations pénales[Article 395 point 1 à 4 du code du numérique] et aux infractions ou aux mesures de sûreté connexes ;

L'APDP se prononce alors dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée du président [Article 411 points 1 à 5 du CDN]

Sont également soumis à autorisation les transferts hors de la CEDEAO [Article 391 alinéa 4]vers le reste du monde.

A l'issue de l'étude du dossier, l'APDP délivre une autorisation de traitement au postulant.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

iii. Les avis [Article 413 du CDN]

L'APDP donne des avis à chaque fois qu'elle est sollicitée

Les traitements automatisés de données à caractère personnel opérés pour le compte de l'Etat, des établissements publics, des collectivités territoriales et des personnes morales de droit privé gérant un service public étaient présumés, requièrent l'avis de l'APDP avant la prise d'un acte réglementaire d'autorisation par le gouvernement si cet avis était réputé favorable au terme d'un délai de deux mois, renouvelable pour un mois une fois.

L'avis de l'Autorité est publié avec le décret autorisant ou refusant le traitement.

L'acte d'autorisation est donné par décret pris en conseil des ministres après avis favorable de l'APDP.

vi. Les plaintes [Article 481 du CDN]

L'Autorité traite également des plaintes en cas par exemple du refus d'un droit quelconque des personnes concernées par des traitements (cas de refus de droit d'accès ou d'un droit de rectification et de suppression) ou d'un citoyen dont les données personnelles sont exploitées sans son consentement ou de plaintes d'une société contre l'Etat

9. PRINCIPE DE TRAITEMENT DONNEES PERSONNELLES

- **Les traitements sur les données personnelles devront obéir à 7 principes :**

1) Le principe de licéité, loyauté et transparence ;

La loi impose que les données soient collectées et traitées de manière loyale et licite, dictant donc de manière implicite au responsable du traitement une transparence absolue dans le traitement des personnes concernées par le traitement.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

Autrement dit :

- La loi garantit aux personnes ayant soumis leurs données, l'information nécessaire relative aux traitements les concernant ;

- Elle les rassure de la possibilité d'un contrôle personnel ;

- Le responsable du traitement de données personnelles a l'obligation d'avertir ces personnes dès la collecte des données et en cas de transmission de ces données à des tiers.

2. Le principe de finalité

- Les données à caractère personnel ne doivent être collectées et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'organisation ou du responsable du traitement. Tout détournement de finalité est passible de sanctions pénales ;

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

3. Le principe de proportionnalité

- La loi exige que les données ne soient collectées que pour un traitement bien spécifique et clairement défini.

Par exemple : dans le cas d'une opération de marketing direct soumise à ce principe où les nom et prénoms et l'adresse email suffisent amplement au traitement envisagé, la collecte pour cette même finalité de l'adresse postale, la situation familiale, financière, etc., sera jugée non proportionnelle et donc coupable d'une sanction

4. Le principe de pertinence des données ;

Les organisations doivent faire en sorte que les données soient exactes et mises à jour si nécessaire.

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

5. Le principe de durée limitée de conservation des données

- Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier. Passée cette limite, les données doivent être supprimées ou rendues anonymes. Toutefois la conservation des données personnelles au-delà du délai de conservation [Article 433 alinéa 3] déclaré doit être soumis à l'APDP

6. Le principe de sécurité et de confidentialité

Le code prévoit un renforcement des mesures de sécurité. Les organisations sont responsables de la sécurité des données qu'elles traitent et doivent mettre en place les mesures adéquates pour la garantir (pseudonymisation des données, analyses d'impact, tests d'intrusion, etc

REGIME DE TRAITEMENT DES DONNEES PERSONNELLES

- Ainsi, le responsable de traitement doit faire prendre les mesuresd e sécurité nécessaires pour :

- Garantir la confidentialité des données et éviter leur divulgation. En d'autres termes, le responsable de traitement doit s'assurer que des tiers non autorisés ne peuvent accéder aux données ;

- Empêcher que les données soient déformées, endommagées ou pyratée
- Des mesures de sécurité, tant physique que logique, doivent donc être prises..

7. Le principe de responsabilité

- Ce principe intègre la responsabilité du responsable du traitement en tant que principe exigeant des organisations qu'elles mettent en place des mesures techniques et organisationnelles appropriées et qu'elles soient en mesure de démontrer ce qu'elles ont fait et son efficacité sur demande.
- Les organisations, doivent démontrer qu'elles se conforment à la loi

❑ 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/