Opérations de traitement et cadre juridique du traitement des données dans les services financiers décentralisés

- **Formation des acteurs du système financier sur la protection des données personnelles**

Qu'est-ce qu'un traitement des données ?

La connaissance gouverne le monde. Aucun projet ne peut se former sans un minimum d'éléments informatifs qui serviront d'intrants pour les déductions, les inductions et les conclusions. Aucune décision ne peut être prise en l'absence de ce déterminant. Il est nécessaire de connaître, de savoir pour élaborer, concevoir.

Cette nécessité implique le recours à de nombreuses informations pour atteindre la plupart des objectifs que l'homme se fixe. C'est donc à raison que diverses informations vont être recueillies, conservées, croisées pour des desseins divers. Ces informations qui servent à identifier une personne ou une chose font donc l'objet de traitement.

C'est dans l'optique d'encadrer ceux de ces traitements qui concernent les informations qui identifient directement ou indirectement une personne que le Code du numérique à consacrer un livre 5ème à la protection des données à caractère personnel en République du Bénin.

Le Code du numérique béninois définit les données à caractère personnel comme 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.

Ainsi, une « **donnée personnelle** » est « **toute information se rapportant à une personne physique identifiée ou identifiable** ».

En tout état de cause, une personne peut être identifiée :

directement

- nom
- prénom
- photo
- vidéosurveillance
- email nominatif
- empreinte digitale
- attribut
- etc

indirectement

- numéro client
- numéro de téléphone
- empreinte digitale
- plaque d'immatriculation
- localisation
- etc

L'identification d'une personne physique peut être réalisée :

à partir d'une seule donnée

- numéro CNSS
- NPI
- Numéro de téléphone

à partir du croisement d'un ensemble de données

- la femme ronde vivant au premier étage de l'immeuble COCODY
- membre de la JCI
- l'homme de teint noir à la voix roque assis sous l'arbre en face de l'école

Aux termes du Code, deux grandes catégories de données à caractère personnel peuvent ainsi être distinguées : les données à caractère personnel ordinaires et les données à caractère personnel soumis à un régime particulier dont les données concernant la santé.

S'il est aisé d'appréhender le concept du traitement grâce à une définition sans ambiguïté fourni par le Code du numérique, le concept de données concernant la santé nécessite que sa théorie soit étayée.

Notion de traitement

Par « traitement », le Code du numérique désigne 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.

Ainsi, 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 diffusion ou toute autre forme de mise à disposition, rapprochement).

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

En somme, les données personnelles sont traitées dès lors qu'elles sont :

Exemples de traitement : Tenue d'un fichier Excel de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, dossier médical, classeurs de dossiers clients etc.

Focus sur le traitement des données financières

Les données financières désignent les informations relatives aux transactions et aux activités financières d'une personne, d'une entreprise ou d'une institution. Ces données comprennent les :

- données d'identification financières (numéros de comptes bancaires, etc.) ;
- les revenus, les possessions, les revenus totaux, les revenus professionnels,
- l'épargne, les dettes, les dépenses (dépenses totales, dépenses pour le loyer, prêts, etc.) ;
- la solvabilité (appréciation des revenus, du statut financier, de la solvabilité) ; allocations, aides ; les détails relatifs à la pension ; etc.

Les données financières peuvent être collectées à partir de différentes sources, telles que les relevés bancaires, les factures, les contrats, les registres comptables, les déclarations fiscales, les rapports financiers, les systèmes de gestion financière, etc.

Les données financières sont essentielles pour prendre des décisions éclairées en matière de gestion financière, d'investissement, de planification budgétaire, de prévisions et d'évaluation de la santé financière. Elles sont utilisées par les individus, les entreprises, les institutions financières, les gouvernements et les régulateurs pour évaluer la performance financière, mesurer les risques, réaliser des analyses financières, déterminer l'admissibilité au crédit, effectuer des audits et répondre aux exigences réglementaires.

La protection des données financières revêt une importance capitale en raison de leur sensibilité et de leur confidentialité. Les données financières peuvent contenir des informations confidentielles, telles que les numéros de compte bancaire, les numéros de carte de crédit, les codes de sécurité, les données fiscales personnelles, etc. La divulgation non autorisée de ces informations peut entraîner des fraudes, des vols d'identité, des abus financiers et d'autres conséquences néfastes pour les personnes ou les entités concernées.

En définitive, la quantité d'informations que les consommateurs fournissent sans en avoir conscience (ou sans y avoir consenti) est en constante augmentation, en raison des évolutions technologiques qui imprègnent tous les aspects de nos sociétés et qui déterminent la génération et la capacité d'analyse de volumes croissants de données de caractère personnel.

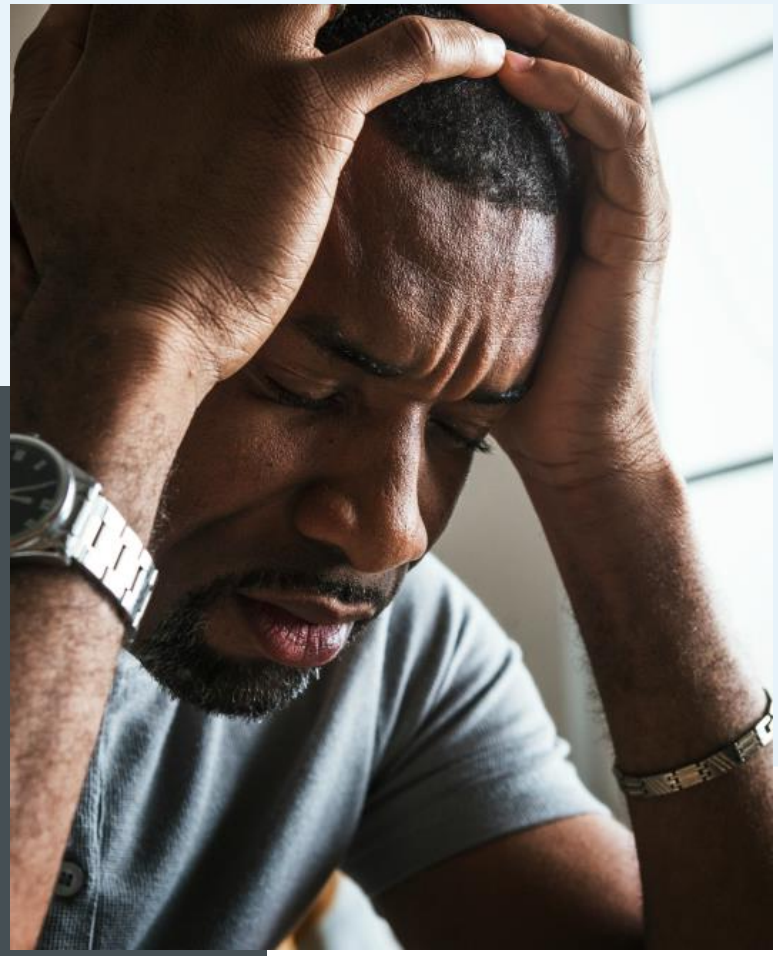
Les flux de données de caractère personnel entre le consommateur et les prestataires de services financiers peuvent être répartis en grandes catégories fondées sur la connaissance que le consommateur a ou non de ces flux.

Généralement les **clients ont connaissance des flux de données** lorsqu'il s'agit de :

- Données fournies par le consommateur lors du processus de vérification de l'identité
- Données transmises par le consommateur à l'appui d'un achat de produit spécifique
- Données transmises par le consommateur pour utiliser un service spécifique comme les outils d'agrégation des données
- Données collectées lorsque le consommateur utilise des produits financiers spécifiques, tels que les services de paiement

Par contre, le **client n'a pas connaissance des flux de données** quand il s'agit de :

- Données collectées par le prestataire lors des interactions avec les clients
- Données collectées par le prestataire à partir de sources d'information accessibles au public (réseaux sociaux)
- Données partagées avec le prestataire par des tiers, tels que les bureaux d'évaluation du risque de crédit



Comprendre l'enjeu

Le soin apporté pour définir cette notion trouve son fondement dans la nécessité d'encadrer juridiquement la réalité.

Pourquoi ?

La connaissance accrue des clients

D’abord parce que les structures financières décentralisées collectent et traitent une quantité considérable d'informations personnelles sensibles, telles que les données financières des emprunteurs, leurs antécédents de crédit, leurs informations démographiques, etc.

N’étudiant jusque-là que des données liées à leur marché pour développer leurs stratégies commerciales, elles ont vite compris l’intérêt de posséder de plus en plus d’informations personnelles sur leurs clients (âge, sexe, géolocalisation, habitudes d’achats, classe socioculturelle…) pour mieux les connaitre, leur proposer des offres de mieux en mieux ciblées et améliorer les scores de recouvrement des créances.

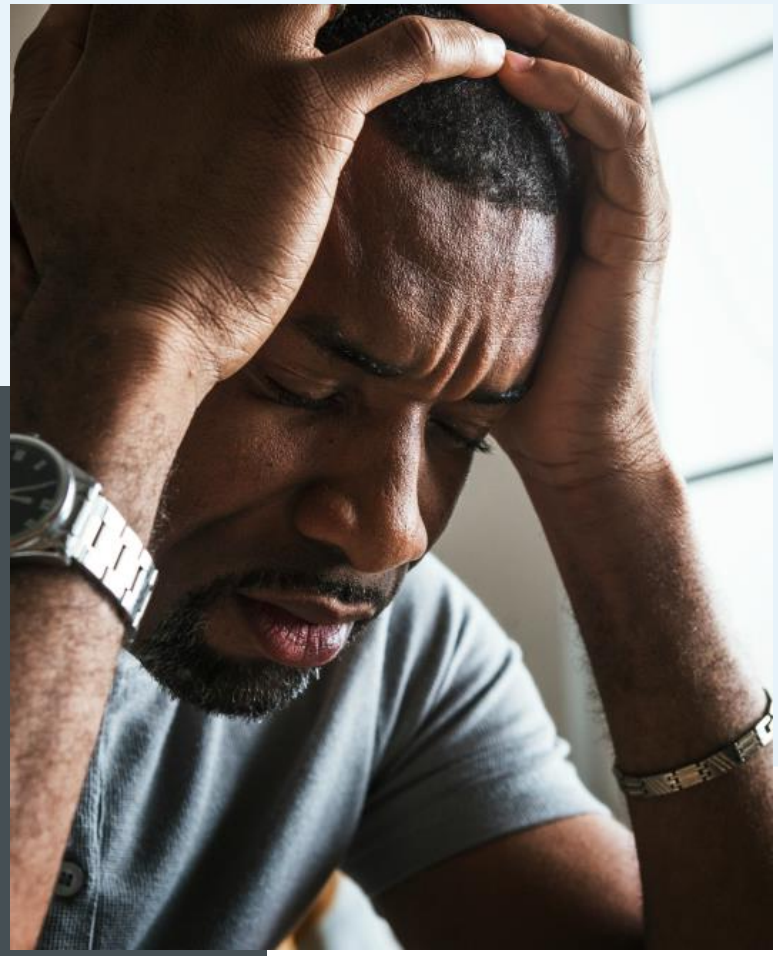
Très vite, elles ont donc mis en œuvre les moyens pour obtenir et maitriser le maximum d’informations sur leurs clients et prospects.

.

Le partage des données

Ensuite parce que, les structures financières décentralisées peuvent être amenées à partager des données avec d'autres partenaires ou prestataires de services, tels que des agences d'évaluation du crédit ou des sociétés de traitement des paiements.

Par exemple, pour stocker les données de leurs clients, beaucoup d’entreprises font appel à des bases de données externes. Les données sont donc souvent stockées physiquement dans des datacenters. Il s’agit classiquement de grands entrepôts avec des salles remplis de serveurs pour héberger les données et les entreprises louent une partie de ces datacenters pour le stockage de leurs données.



Or, le traitement des données dans le secteur des structures financières décentralisées expose à des risques réels

- **de disparition**
- **de vol et**
- **de modification non désirée**

Chacun de ces risques est accompagné d'un lot de conséquences.

La disparition des données

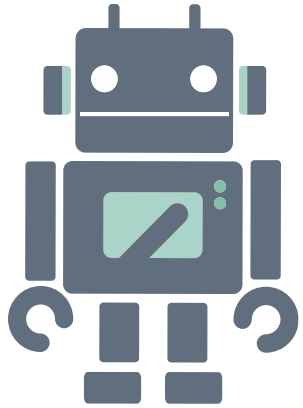
La disparition des données personnelles peut entraîner **une violation de la vie privée des personnes concernées.** Les informations confidentielles telles que les données financières, les antécédents de crédit, les informations d'identification, etc., pourraient tomber entre de mauvaises mains. Cela peut entraîner des atteintes à la vie privée, des fraudes financières, des usurpations d'identité et d'autres formes d'abus.

La disparition des données personnelles peut également entraîner **une perte de confiance des clients** envers les institutions financières concernées. Les clients peuvent craindre que leurs informations personnelles ne soient pas correctement protégées et hésiter à fournir des informations sensibles à l'avenir. **Cela peut nuire à la réputation de l'institution financière et entraîner une diminution de sa clientèle.**

Un vol

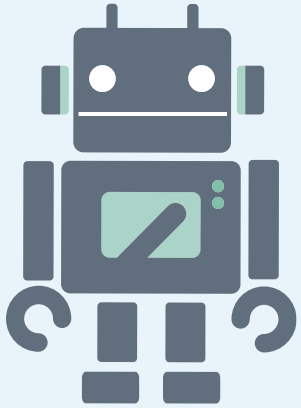
Lorsque des données personnelles sont perdues ou volées, les criminels peuvent les utiliser pour commettre des fraudes financières. Cela peut inclure l'ouverture de comptes frauduleux, l'accès à des comptes bancaires, la réalisation de transactions non autorisées, etc. Les individus touchés peuvent subir des pertes financières importantes et avoir des difficultés à rétablir leur situation financière.

L’altération



L'altération des données personnelles peut entraîner la divulgation non autorisée d'informations sensibles, telles que les numéros de compte, les informations d'identification personnelle, les antécédents de crédit, etc. Cela peut ouvrir la voie à des cas de fraude, d'usurpation d'identité et de vol d'argent, ce qui porte atteinte à la confidentialité financière des personnes concernées. Ces situations peuvent entraîner des pertes monétaires considérables. Les personnes victimes d'altération de données peuvent subir des dommages financiers à long terme en raison de l'usurpation de leur identité et des répercussions négatives sur leur historique de crédit.

L’altération



De plus, l'altération des données personnelles peut avoir un impact plus large sur l'économie dans son ensemble. Si la confiance dans le système financier est ébranlée en raison de l'altération des données, cela peut entraîner une réduction de l'investissement, de la consommation et de la croissance économique globale.

C’est pourquoi, renforcer leur protection à travers un cadre juridique spécifique est devenu un enjeu majeur de la cybersécurité au cours des dernières années. Il est notamment important, dans le cadre de tout traitement, de s’assurer que les données bénéficient de :

La confidentialité

L’intégrité,

La disponibilité et

La traçabilité des traitements dont elles font l’objet

Les opérations de traitement conformément aux exigences du livre 5ème

Le traitement des données à caractère personnel au Bénin est conforme aux exigences règlementaires seulement dès lors qu'il respecte les principes de traitement édictés par le code du numérique, garantit aux personnes concernées leurs droits, s'effectue par un responsable du traitement effectivement responsable et assurant une bonne gouvernance des données.

Les principes de traitement des données à caractère personnel

Trois grands principes

3 doivent gouverner en tout au traitement des données à caractère personnel. Il s'agit des principes de :

licéité

transparence

confidentialité et sécurité.

Le principe de licéité des traitements de données à caractère personnel

Un traitement licite est un traitement consenti dont la finalité est déterminée, explicite et connue de la personne concernée avant sa mise en œuvre, qui est loyal et pertinent tout en se servant de données exactes.

Le principe du consentement

qui veut dire que le traitement des données à caractère personnel doit toujours être légitime. Cette légitimité doit alors être tirée du consentement de la personne concernée, de l'ordre de la loi ou de la poursuite et l'atteinte d'un intérêt public. Autrement dit :

- **pas de traitement si la personne concernée n'a pas dit oui,**
- **pas de traitement sauf si la loi exige le traitement en question que la personne concernée ait dit oui ou pas,**
- **pas de traitement sauf si la poursuite d'un intérêt public le rend nécessaire, que la personne concernée ait dit oui ou pas.**

Le principe de loyauté

qui se manifeste entre autres à l'occasion de l'information des personnes lors de la collecte des données, autant que lors de l'exercice potentiel du droit d'opposition des personnes sur les données qui les concernent. Le principe interdit que des données soient recueillies des personnes ou conservées par malice ou par fraude.

Il est par exemple déloyal d'équiper un téléphone d'une caméra qui filme l'utilisateur à son insu ou même quand le téléphone est éteint.

De même le chargé de prêt qui se sert des données de sa cliente pour faire une étude de marché est déloyal.

Le principe de finalité

qui exige que le traitement ait une raison d'être connue, c'est-à-dire déterminée et que soit mis à disposition des personnes dont les données sont traitées, un certain nombre d'informations dont :

- **La ou les raison(s) pour laquelle/lesquelles, elles doivent fournir leurs données,**
- **Ce que leurs données serviront à faire ;**
- **La durée durant laquelle leurs données seront conservées ;**
- **Les personnes qui manipuleront leurs données.**

De même, si ce principe exige que le traitement qui sera fait des données recueillies sur la base d'une finalité ne change pas et que les mêmes données ne soient pas traitées pour une finalité différente.

En d'autres termes, **le chargé de crédit qui se sert des données de ses clients pour des fins de mise en relation avec des usuriers** commet une violation du principe de finalité en raison du détournement de la finalité initiale pour laquelle il a traité ses données sont obtenues.

Le principe de pertinence

qui veut que pour un traitement donné, il ne soit pas recueilli plus de données qu'il n'est utile. Le principe prône la minimisation des données recueillies au regard des objectifs poursuivis par le traitement.

L'application mobile de jeu qui demanderait à prendre mon pouls pendant que je l'utilise ne compte certainement pas améliorer mon expérience utilisateur.

Le principe d'exactitude

qui exige que toutes les mesures raisonnables soient 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.

En effet, un nom mal orthographié sur votre carte nationale d'identité peut vous empêcher l'accès à votre bureau (cas d'un bureau sécurisé par un contrôle d'accès automatique), à votre compte bancaire (pour des opérations de retrait par exemple), au droit de vote etc.

De même, un diagnostic erroné peut avoir des effets néfastes.
Le principe d'exactitude démontre tout son sens en ce que l'inexactitude des données personnelles traitées par un organisme peut affecter la jouissance de droits ou de faveurs à la personne concernée.

Il faut noter enfin que **la licéité est non seulement un principe sacro-saint du traitement des données à caractère personnel mais aussi la condition nécessaire à tout traitement.**

Le principe de la transparence

Aux termes de **l'article 384 du Code du numérique, le principe de transparence implique une information obligatoire et claire ainsi qu'intelligible de la part du responsable du traitement.**

Lorsque les données personnelles sont collectées auprès de la personne concernée, il est obligatoire que le responsable du traitement ou son représentant fournisse à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, au moins les informations relatives à son identité et l'adresse de sa résidence habituelle ou de l'établissement principal et, le cas échéant, les coordonnées de son représentant ou du délégué à la protection des données.

Lorsque le traitement est fondé sur les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, il doit l'informer par rapport aux finalités déterminées du traitement auquel les données sont destinées.

Il doit aussi l'informer sur les destinataires auxquels les données sont susceptibles d'être communiquées, sur ses droits entre autres, d'opposition, de refus de figurer sur le fichier, d'accès et de rectification aux données de réclamation etc.

Code du numérique

Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement ou son représentant, doit selon le délai prévu par la loi, donner à la personne concernée les informations prévues à **l'article 416** du Code du numérique.

Le principe de confidentialité et de sécurité

Code du numérique

Conformément à **l'article 385 du Code du numérique, le traitement des données à caractère personnel est obligatoirement confidentiel.** Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions, sauf en vertu d'obligations légales contraires.

Afin de garantir **la sécurité des données** à caractère personnel, **des mesures techniques et d'organisation appropriées** doivent être mises en œuvre **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.

Le respect des principes est contrôlé au moment de se soumettre à l'un ou l'autre régime de traitement des données.

Les régimes juridiques de traitement des données à caractère personnel

La mise en œuvre des opérations de traitement est soumise à la souscription à l'un des trois régimes de traitement édictés par la loi. Il est en effet prévu un régime de déclaration préalable un régime d'autorisation et un régime d'avis auprès de l'Autorité de Protection des Données à caractère Personnel -APDP.

Déclaration préalable

Code du numérique

Aux termes de **l'article 405 du Code du numérique, une déclaration préalable est requise pour le « les traitements automatisés ou non automatisés exécutés par des organismes publics ou privés et comportant des données à caractère personnel ».** Un formulaire est disponible en ligne sur le site de l'Autorité pour faciliter la déclaration des diverses opérations de traitement par les responsables de traitement.

La déclaration est prescrite pour les traitements des données à caractère personnel autres que ceux portant sur les données soumises à régime particulier. Les traitements effectués à partir d'un site web ou d'une caméra de vidéosurveillance sont soumis à ce régime.

La déclaration est nécessairement préalable et doit être suffisamment documentée pour permettre à l'Autorité de contrôler le respect des principes de traitement et des exigences imposées au responsable de traitement.

Autorisations

Selon **l'article 407 du Code du numérique une demande d'autorisation doit être présentée par le responsable du traitement ou son représentant à l'APDP préalablement au traitement dans les cas suivants :**

- **Traitements déterminés par l'APDP ;**
- **Données sensibles et DCP aux fins de journalisme et d'expression littéraire et artistique ;**
- **Actes d'identité tels que l'ANIP, l'IFU, le passeport etc. ;**

- **Données biométriques ;**
- **Traitements aux fins historiques, statistiques et scientifiques ;**
- **Interconnexion de fichiers ;**
- **Transferts de données hors CEDEAO ;**
- **Traitements automatisés relatifs aux difficultés sociales des personnes.**

La demande d'autorisation est donc systématiquement prescrite dans le cadre d'un traitement portant sur des données concernant la santé.

La demande d'autorisation peut être adressée à l'Autorité par voie électronique ou par voie postale ou par tout autre moyen contre remise d'un accusé de réception par l'Autorité.

Elle doit au moins contenir :

1. l'identité, l'adresse complète ou la dénomination sociale du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire de la République du Bénin, les coordonnées de son représentant dûment mandaté ;

2. la ou les finalités du traitement ainsi que la description générale de ses fonctions ;

3. les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;

4. les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5. la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;

6. le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7. les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8. la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

9. les dispositions prises pour assurer la sécurité des traitements et des données dont les garanties qui doivent entourer la communication aux tiers ;

10. l'indication du recours à un sous-traitant ;

11. les transferts de données à caractère personnel envisagés à destination d'un État tiers, sous réserve de réciprocité ;

12. l'engagement que les traitements sont conformes aux dispositions du présent Livre.

Avis

Selon l'article 411 du Code du numérique, « … Les traitements des données à caractère personnel opérés pour le compte de l'État, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont autorisés par décret pris en Conseil des ministres après avis motivé de l'Autorité. Ces traitements portent sur :

a. La sûreté de l'État, la défense ou la sécurité publique ;

b. La prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

c. Le recensement de la population ;

d. Les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;

e. Le traitement de salaires, pensions, impôts, taxes et autres liquidations… »

La gouvernance responsable des données

Le Code du numérique procède à la responsabilisation des organismes, c'est-à-dire de toute personne physique ou morale qui décider de traiter des données à caractère personnel : c'est **« l'accountabilty »** qui se traduit par une gouvernance responsable des données.

La gouvernance responsable ou « accountable » devrait permettre de mettre en place des procédures qui garantissent la protection des données à tout instant, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement tel que :

- **faille de sécurité,**
- **gestion des demandes de rectification ou d'accès, modification des données collectées,**
- **changement de prestataire.**

Cela se traduit notamment par la réalisation d'**analyse d'impacts, la protection des données dès la conception et par défaut,** la tenue d'un **registre des traitements,** la désignation d'un **délégué à la protection des données** et la formation/sensibilisation du personnel.

L’analyse d’impact relatif à la protection des données (AIPD)

Une étude d'impact est une réflexion collective qui vise à apprécier les conséquences de toutes natures, d'un projet pour tenter d'en limiter, atténuer ou compenser les impacts négatifs.

L’analyse d’impact est exigé par le Code du numérique à l’article 428 lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Ainsi, **le 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 nécessite la réalisation d’une analyse d’impacts.

Une analyse d’impact doit être obligatoirement réalisée lors que le traitement entraine un risque élevé pour les droits et libertés des personnes concernées.

Par droits et libertés, il faut entendre non seulement le droit au respect de la vie privée mais également les autres droits fondamentaux, tels que la liberté de circulation, la non-discrimination, le droit à la vie etc. L'AIPD doit être effectuée avant la mise en œuvre du traitement. Ainsi, répondra-t-elle aux principes de privacy by design et de privacy by default. Elle a pour vocation de permettre au responsable du traitement d'élaborer des mesures protectrices avant même la mise en œuvre du traitement.

Le Privacy by Design and by default

Concept fut créé au Canada dans les années quatre-vingt-dix par Ann CAVOUKIAN Ph. dans le cadre de ses fonctions de Commissaire à l'information et à la protection de la vie privée de l'Ontario, **le Code du numérique consacre la notion en droit béninois notamment en son article 424.**

Il s'agit à travers ce concept, d'anticiper toutes les dérives potentielles et les risques d'exploitations abusives des données.

La démarche permet de réaliser des projets informatiques de sorte à protéger les données à caractère personnel des personnes concernées par lesdits projets, mais également de protéger le droit à la vie privée. Elle impose d'intégrer à toute technologie exploitant des données à caractère personnel des dispositifs techniques de protection de la vie privée dès sa conception et de s'y conformer tout le long du cycle de vie des données.

Surtout, cette notion est non seulement le préalable et nécessaire à toute logique de conformité mais aussi utile pour éviter de concevoir des solutions peut être innovantes, mais inutiles à la fin parce qu'elles seraient violatrices de la vie privée et attentatoires aux données à caractère personnel.

La notion peut se décliner ainsi qu'il suit :

1. **La protection doit être à priori et pas à posteriori** (Article 424 al 1 CDN)
2. **La confidentialité doit être paramétrée par défaut** (Article 424 al 2 et 425 CDN)
3. **La confidentialité doit être intégrée à la conception** (Article 424 CDN)
4. **Les fonctionnalités doivent être fournies intégralement selon un paradigme à somme positive et non à somme nulle.** (Article 428, 429 CDN)
5. **La sécurité doit être prise en compte de bout en bout et pendant tout le cycle de vie du produit** (Articles 426, 433,434, 435 CDN)

6. **La transparence doit toujours régnée** (Article 418-423-415-416-437-443-410 CDN)
7. **La confidentialité doit être centrée sur les besoins des utilisateurs** (Article 424 al 2 et 425 CDN)

La tenue du registre de traitement

Le registre est un outil de gouvernance qui donne une vue d'ensemble sur les activités de traitement de l'organisme.

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.

Le registre comporte toutes les informations suivantes **(article 435 du Code du numérique)**

- **Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;**
- **Les finalités du traitement ;**

- **Une description des catégories de personnes concernées et des catégories de données à caractère personnel ;**
- **Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;**
- **Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale ;**
- **Les délais prévus pour l'effacement des différentes catégories de données ;**
- **Une description générale des mesures de sécurité techniques et organisationnelles.**

Pour éclairer la pratique, l'Autorité a publié sur son site www.apdp.bj , un modèle de registre qui peut être personnalisé par les responsables du traitement ou servir de point de repère.

La désignation d'un délégué à la protection des données

Aux termes de **l'article 430 du Code du numérique, « le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données … 3. les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 394 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395. ».**

Cette désignation va témoigner de la volonté du responsable de traitement d'opérer ses traitements dans le respect des prescriptions légales. En se dotant d'un délégué à la protection des données à caractère personnel ou **DPO,** le responsable du traitement, s'« équipe » d'un « œil » du Code et de l'Autorité dans son organisme. C'est une présomption suffisante de son engagement à être responsable.

La mission principale d'un DPO est de faire en sorte que l'organisme qui l'a désigné soit en conformité avec le cadre légal relatif aux données personnelles.

La fonction de DPO apparait donc comme un élément clé de co-régulation par la pratique. D'ailleurs, le positionnement du DPO dans l'organisme est un facteur crucial de son efficacité et de la portée des actions.

Indépendant, il est le point de contact entre l'Autorité et l'organisation. Pour autant, précisons que le DPO n'est pas responsable de la conformité au Code du numérique. Cette responsabilité est portée par le responsable de traitement. Toutefois, il est essentiel que le DPO soit libre et indépendant pour mener sa mission, il ne doit pas être placé en situation de conflits d'intérêts.

Le choix du DPO doit prendre en compte un certain nombre de critères de compétences et d'éthique. Il doit, à l'évidence, maîtriser tous les enjeux liés à la protection des données personnelles en général, et au Code du numérique en particulier. Il peut être membre de l'entreprise ou agir en qualité de prestataire externe (cabinet de consulting…).

Troisième exigence du principe d'accountability de l'article 387 du Code du numérique, le responsable de traitement doit « informer les personnes agissant sous son autorité des dispositions du présent Livre et de ses textes d'application, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel ».

Cette information vise notamment à **informer sur les fondamentaux relatifs à la protection des données à caractère personnel** de sorte à ce que chaque salarié comprenne les notions de protection et se sente concerné.

La formation doit se faire continuellement. Dans le guide de rédaction des rapports annuels publié par l'APDP sur son site, le point D intitulé DIFFUSION DE LA CULTURE DE LA PROTECTION DES DONNEES PERSONNELLES interroge sur le nombre de sessions de sensibilisation/formations réalisées, nombre d'heures en moyenne par session et sur la fréquence d'organisation de sessions de formation comme pour insister sur la sacralité de l'action de sensibilisation continue.

L'obligation peut être satisfaite :

- **sous forme de réunions de sensibilisation dont il faudra conserver les preuves,**
- **sous forme de renforcement de capacités,**
- **sous forme de formation continue,**
- **une campagne de communication visuelle par affichages,**
- **dépliants,**
- **pop-ups sur l'intranet de l'organisme,**
- **courtes vidéos thématiques etc.**

Tout moyen est bon pour faciliter l'assimilation des messages en termes de protection des données et obtenir une large adhésion des différents acteurs.

Les nouveaux arrivants pourraient même être invités à une formation initiale sur le sujet dans leur parcours d'intégration.

Enfin, il faut garder à l'esprit, que ces séances de sensibilisations ou de formations seraient plus faciles à prouver si elles sont sanctions par des attestations de suivi.

Le choix du sous-traitant

Au sens du Code du numérique, **le sous-traitant est défini comme 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 donc toute personne autre que le destinataire connu ou supposé des données mais l'ayant reçu par le biais de ce dernier afin d'atteindre des objectifs que ce même lui a fixé.

Autrement dit, le sous-traitant c'est :

- **L'intégrateur web externe**
- **L'application de gestion d'une ou partie des traitements**
- **Le concepteur externe de base de données**
- **Le prestataire de services de numérisation de documents**
- **Le prestataire de services d'archivage**
- **L'hébergeur web**
- **L'agence marketing**
- **Le fournisseur de solutions de stockage cloud**
- **Le propriétaire du système d'informations interne etc.**

L'article 386 du Code guide sur les critères qui doivent entrer en ligne de compte au moment de choisir son sous-traitant.

Il dispose en effet que « …lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en République du Bénin, doit : 1. choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements, notamment pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, de manière à ce que le traitement réponde aux exigences du présent Livre et garantisse la protection des droits des personnes concernées… ».

Il est donc nécessaire de procéder à une approche globale de l'évaluation d'un sous-traitant, tenant d'abord compte des exigences du Livre 5ème vis-à-vis de lui.

Parmi elles, on dénombre :

- **La présence d'un DPO ;**
- **La formation/sensibilisation de ses salariés aux enjeux de la protection des données personnelles ;**
- **L'existence de registre de procédure de gestion des registres et des traitements ;**
- **La gestion et le contrôle de la conformité des sous-traitants ultérieurs ;**
- **La localisation du traitement des données personnelles ;**
- **Le transfert de données personnelles hors CEDEAO ;**
- **Les mesures techniques de protection des données personnelles ;**
- **Les mesures organisationnelles de protection des données personnelles ;**
- **La gestion des droits des personnes ;**
- **La prise en compte des principes de protection des données « Privacy by design » et « Privacy by default » ;**

- **L'adhésion à un code de conduite ;**
- **L'obtention d'une certification.**

D'un **point de vue opérationnel,** le responsable de traitement devrait établir un questionnaire contenant toutes les informations qu'il juge utiles pour s'assurer que le sous-traitant présente des garanties suffisantes et intégrer l'usage de ce questionnaire dans un process interne relatif au choix d'un nouveau prestataire.

- **Avez-vous désigné un Délégué à la Protection des Données ?**
- **Avez-vous établi un registre des activités de traitement Responsable de traitement et Sous-traitant ?**
- **Avez-vous une Politique de Sécurité ?**
- **Avez-vous mis en place une procédure de gestion de crise, notamment en cas de violation de données ?**
- **Votre personnel est-il formé/sensibilisé à la protection des données ?**

En analysant les réponses obtenues, le responsable de traitement sera en mesure de faire une présélection des sous-traitants, pour ne retenir que ceux démontrant un bon niveau de maturité en matière de protection des données.

Par ailleurs, il est souvent constaté dans les modèles de contrats fournis par les sous-traitants qu'ils se réservent la possibilité de faire eux-mêmes appel à un sous-traitant de second rang afin de déléguer une partie des opérations de traitement.

Si bien souvent le contrat contient l'obligation pour le sous-traitant d'en informer au préalable le responsable de traitement pour lui permettre d'émettre des objections, dans les faits ce dernier en a rarement connaissance.

Il est donc fortement recommandé que le responsable de traitement prenne en compte la chaine de sous-traitance au moment de sélectionner un sous-traitant et de bien l'encadrer contractuellement.

Si l'audit n'est pas obligatoire, ce dernier reste un instrument efficace permettant l'assurance du maintien de la visibilité des pratiques du sous-traitant. Il est ainsi fortement conseillé de mettre en pratique régulièrement une clause contractuelle d'audit (au moins une fois par an).

Si aucun des points ci-dessus ne permet à lui seul d'apprécier « les garanties suffisantes », cela constitue néanmoins un faisceau d'indices qui peut être utilisé pour faire une présélection des sous-traitants.

Merci