COMMENT STRUCTURER UN PROGRAMME DE MISE EN CONFORMITE ?

Autorité de Protection des Données Professionnelles
Formation des DPO du 29 novembre au 02 Décembre 2021

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

Table des matières

1. CONTEXTE

➢La question de la protection des données personnelles et de la vie privée est au cœur des enjeux et des débats sociopolitiques contemporains;

➢ Les pratiques de collecte, d'exploitation et de conservation des données personnelles font partie des modes d'administration des populations, des caractéristiques des **« sociétés de contrôle** » et des modèles économiques;

➢ A l'ère de la « **globalisation de la surveillance** », les technologies de l'information et de la communication (TIC) ont contribué à généraliser, dans les secteurs privé et public, des pratiques de collecte systématique et d'exploitation des données personnelles et des traces des individus à des fins diverses;

➢ Indissociables des TIC, les enjeux résident désormais dans les modes de protection des données personnelles mis en œuvre au niveau des Etats. Ils se matérialisent à travers des textes de lois, des techniques, d'acteurs, de politiques et de pratiques en interrelation.

II. MISE EN CONFORMITE A LA LOI SUR LA PROTECTION DES DONNEES PERSONNELLES

- Tout organisme public ou privé collectant des données personnelles est astreint à se conformer à la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin

- Pour mener à bien cette conformité, certaines activités essentielles doivent être menées dont les plus importantes entre autres sont les suivantes :

  - **Recenser** l'ensemble des traitements de données dans un registre des activités de traitement ;

  - **Faire le tri de toutes données** pour vérifier si les données en traitement sont nécessaires à l'activité menée et que celles sensibles en sont exclues et si elles ne le sont pas, s'assurer de disposer des autorisations prescrites par la loi

II. MISE EN CONFORMITE A LA LOI SUR LA PROTECTION DES DONNEES PERSONNELLES

- **S'assurer du respect des droits des personnes dont les données sont traitées ;**
- **S'assurer que données des personnes concernées par le traitement sont sécurisées.**

III. Les enjeux de la conformité à la loi

Les enjeux sont triples :

- ❑ Créer la confiance entre les parties prenantes ;
- ❑ Sécuriser les données personnelles ;
- ❑ Et responsabiliser les acteurs et les sous-traitants

IV. PROGRAMME DE MISE EN CONFORMITÉ À LA LOI

i. Sensibiliser

Sensibiliser et informer chaque collaborateur des fondamentaux de la loi pour que la mise en conformité se fasse le plus efficacement possible;

ii. Etat des lieux

Réaliser la cartographie de l'ensemble de tous les traitements mis en œuvre.

Elle va permettre de mesurer l'impact de la loi sur l'activité de l'organisme.

l'APDP a mis en ligne un **modèle de registre des activités de traitement** à renseigner [www.apdp.bj]

NB: Porter une attention particulière au fondement de licéité [Art. 383 du CDN] des traitements et à l'âge des personnes concernées. [notamment sur les conditions de traitement des données enfants mineurs]

La tenue d'audit, tant techniques que juridiques, permet de déterminer le niveau de conformité de l'organisme et documenter sa mise en conformité.

La cartographie et les audits permettent également d'identifier les risques.

IV. PROGRAMME DE MISE EN CONFORMITÉ À LA LOI

iii. Identifier et gérer les risques

La loi introduit un nouvel outil de gestion des risques, à savoir l'**analyse d'impact relative à la protection des données** (en anglais, *Data Protection Impact Assessment* ou DPIA).

Le registre des activités de traitement ainsi que les audits sont des outils importants lorsque le responsable du traitement effectue un DPIA.

Bien que le DPIA ne soit obligatoire que dans certains cas, il permet de recenser les mesures protectrices et/ou correctives mises en place pour chaque traitement et d'évaluer la gravité des risques [**Article 428 point 1 à 3 du CDN**]

iv. Assurer les droits des personnes

Les personnes concernées par le traitement ont de nouveaux droits sous la nouvelle loi [droits à la portabilité des données, à la limitation du traitement , à l'effacement, à l'oubli, etc...] Pour chaque nouveau droit, il convient de prévoir une procédure correspondante assurant l'exercice effectif de ce droit. Pour rappel, toute demande d'exercice d'un droit de la part d'une personne concernée doit obtenir une réponse dans les délais raisonnables fixés [Article 420 du CDN] par la loi.

IV. PROGRAMME DE MISE EN CONFORMITÉ À LA LOI

Réaliser la revue documentaire

- Repenser l'approche de la protection des données personnelles à la lumière du principe **<u>d'ACCOUNTABILITY</u>** [**mise en œuvre des mécanismes et procédures internes démontrant le respect des règles relative à la protection des données**] *qui* est l'un des principaux piliers de la conformité.
- Être en mesure de démontrer leur conformité par le biais de divers documents (ex : politique de protection des données, registre des activités de traitement etc…);
- Actualiser l'ensemble des documents, procédures ou mesures existantes au regard des exigences de la loi (ex : bandeau cookie, contrats de prestataires, politique cookies…)..
- Garder à l'esprit les changements qu'apporte la loi au consentement qui doit être libre, spécifique, éclairé et ne peut résulter d'une manifestation tacite.
- Incorporer la protection des données à caractère personnel dès la conception et par défaut (***notions de privacy by design et privacy by default***) [Article 424 du CDN] toute mesure de protection ou procédure doit

IV. PROGRAMME DE MISE EN CONFORMITÉ À LA LOI

vi. Revoir la relation avec le sous-traitant

- Repenser les relations contractuelles avec le ou les sous-traitants dans le respect des exigences de la loi également astreints aux obligations en matière d'*accountability* et de sécurité des données au même titre que le responsable de traitement;
- Faire figurer dans le contrat les dispositions non-limitatives de l'**article 386 du CDN**. Ces derniers sont libres d'ajouter d'autres clauses tant pour les droits que pour les obligations;
- Réviser la clause de responsabilité avec le sous-traitant.

vii. **Implémenter de nouvelles procédures**

- Vérifier qu'elle dispose de procédures permettant aux personnes concernées d'exercer effectivement leurs droits;
- Revoir toutes les mentions d'information afin de s'assurer qu'elles exposent clairement et simplement les droits ainsi que la manière de les exercer;
- Mettre en œuvre des procédures lors d'une violation de données à caractère personnel.

IV. PROGRAMME DE MISE EN CONFORMITÉ À LA LOI

viii. Organiser les procédures de révision

Prévoir des procédures de révision régulières de tous les documents ou procédures portant sur la protection des données à caractère personnel (ex : firewall, politique cookies, procédure de gestion des droits…). En outre, une révision régulière de la documentation permettra à l'entité d'adopter les bons réflexes et d'anticiper une potentielle violation de données à caractère personnel

ix. Désigner un Délégué à la Protection des Données

- Le Délégué à la protection des données (en anglais *Data Protection Officer* ou DPO) est un **acteur indépendant**, dont la désignation est obligatoire. Il est le **chef d'orchestre** de la conformité de l'organisme l'ayant désigné. A ce titre, il doit être associé à toutes les questions relatives à la protection des données à caractère personnel.

IV. PROGRAMME DE MISE EN CONFORMITÉ À LA LOI

x. Niveau international

L'organisme qui transfère des données hors CEDEAO/UEMOA doit prévoir des garanties supplémentaires et s'assurer que le transfert respecte scrupuleusement les conditions imposées par la loi. [**Art. 391 et 392 du CDN]**

V. LES OUTILS DE LA CONFORMITE

- Le Livre Vème du Code du CND offre une boîte à outils diversifiée pour permettre aux organismes de gérer leur conformité [**registre des traitements, mentions d'information, analyses d'impact sur la protection des données, encadrement des transferts, référentiels, certifications ou codes de bonne conduite**] .

5.1. **Le registre des activités de traitement**

Il permet de recenser les traitements de données et de disposer et d'avoir vue d'ensemble de ce qui est fait des données personnelles.

- le registre doit refléter la réalité des traitements de données personnelles effectués et permettre d'identifier précisément :
  - **les parties prenantes** (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ;
  - **Les catégories de données traitées ;**
  - à quoi servent les données, qui sont ceux qui y accèdent et à qui elles sont communiquées ;
  - la durée de conservation et la sécurité des données.

V. LES OUTILS DE LA CONFORMITE

5.2. Contenus d'un registre

- Le registre [**Art 435 du CND**] permet de recenser tous les traitements de données et de disposer d'une vue d'ensemble sur tous les traitements de données personnelles éffectués.
- Un outil de pilotage et de démonstration de la conformité de l'organisation à la loi.
- Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard de la loi pour en déduire un plan d'action de mise en conformité des traitements aux règles de protection des données.
- Il doit refléter la réalité des traitements de données personnelles et permettre d'identifier précisément :
  - **Les parties prenantes** (Responsable de traitement, représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ;
  - Les **finalités** du traitement, l'objectif en vue duquel les données sont collectées ;
  - Les catégories **de personnes concernées** (client, prospect, employé, etc.) ;

V. LES OUTILS DE LA CONFORMITE

- Les catégories de **données personnelles** (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.) ;
- **Les catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels il est fait recours;
- Les **transferts** de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties exigibles prévues pour ces transferts ;
- Une **description générale des mesures de sécurité** techniques et organisationnelles mises en œuvre ;
- **La durée de conservation** des différentes catégories de données, ou à défaut les critères permettant de le déterminer ;

V. LES OUTILS DE LA CONFORMITE

Pour faciliter la tenue de ce registre, l'APDP propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier, permettant de satisfaire au socle d'exigences de la loi .

Modèle de registre simplifié CNIL-FRANCE

Registre de l'APDP

REGISTRE.ods

Registre des activités de traitement_APDP.xl

V. LES OUTILS DE LA CONFORMITE

5.3. Méthode de renseignement du registre

i) Rassembler les informations disponibles

Pour ce faire :

- Identifier et rencontrer les responsables opérationnels des différents services susceptibles de traiter des données personnelles ;
- Si l'organisme dispose d'un site internet, l'analyser et identifier les données collectées dans les formulaires en ligne (questionnaire, formulaire de contact, création d'un compte, etc.), les mentions d'information « protection des données », l'utilisation de cookies, etc.

ii. Elaborer la liste des traitements

- Lister dans un tableau de suivi, les différentes activités de traitement de l'organisme nécessitant le traitement de données personnelles. Les traitements de données doivent être identifiés par finalité et non par logiciel utilisé, car un même logiciel peut être utilisé pour différents traitements et inversement ;

V. LES OUTILS DE LA CONFORMITE

- Sur la base des informations collectées lors des entretiens, remplir une fiche de registre par activité.

  i) **Affiner / préciser**

- Sur la base du registre ainsi renseigné, identifier et analyser les risques qui pourraient peser sur les traitements de données mis en œuvre et élaborer un plan d'actions de mise en conformité à la loi.

VI. ETUDE D'IMPACT SUR LA VIE PRIVEE (PRIVACY IMPACT ASSESSMENT- PIA) et CARTOGRAPHIE

- La démarche de conformité mise en œuvre en menant un PIA repose sur deux piliers :

  i. **les principes et droits fondamentaux** « non négociables », qui sont fixés par la loi et devant être respectés, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;

  ii. la gestion des risques sur la vie privée qui permet de déterminer les mesures techniques et organisationnelles appropriées pour protéger les données.

- Pour mener un PIA, il convient de :

i. **délimiter et décrire le contexte** du(des) traitement(s) considéré(s) ;

ii. **analyser les mesures** garantissant le respect des principes fondamentaux : la proportionnalité, la nécessité du traitement, et la protection des droits des personnes concernées ;

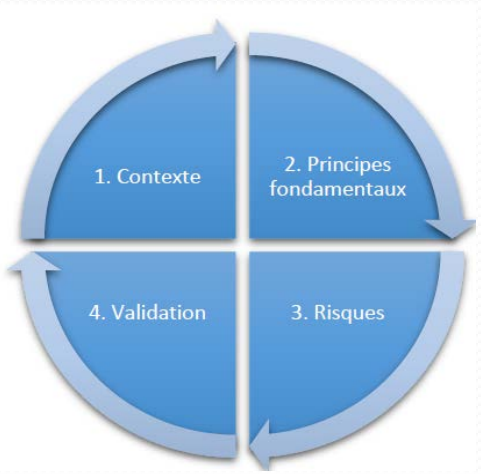
iii. apprécier les risques sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;

iv. **formaliser la validation du PIA** au regard des éléments précédents ou bien décider de réviser les étapes précédentes

VI. ETUDE D'IMPACT SUR LA VIE PRIVEE (PRIVACY IMPACT ASSESSMENT- PIA) et CARTOGRAPHIE

Il s'agit d'un processus d'amélioration continue qui requiert donc parfois plusieurs itérations pour parvenir à un dispositif de protection de la vie privée acceptable. Il requiert en outre une surveillance des évolutions dans le temps (du contexte, des mesures, des risques, etc.), par exemple tous les ans, et des mises à jour dès qu'une évolution significative a lieu.

- La démarche devrait être employée dès la conception d'un nouveau traitement de données à caractère personnel. En effet, une application en amont permet de déterminer les mesures nécessaires et suffisantes, et donc d'optimiser les coûts. A contrario, une application tardive, alors que le système est déjà créé et les mesures en place, peut remettre en question les choix effectués. La méthode générale de réalisation d'un PIA se présente comme suit



VI. ETUDE D'IMPACT SUR LA VIE PRIVEE (PRIVACY IMPACT ASSESSMENT- PIA) et CARTOGRAPHIE

- **6.1. Étude du contexte**

1. Objectif

- obtenir une vision claire des traitements de données personnelles considérés.

2. Vue d'ensemble

i. Présenter le **traitement** considéré, sa **nature,** sa **portée,** son **contexte,** ses **finalités** et **enjeux** de manière synthétique **;**

ii. Identifier le **responsable du traitement** et les éventuels **sous-traitants. ;**

iii. Recenser les **référentiels applicables** au traitement, utiles ou à respecter notamment les codes de conduite [cf. article **414 du CDN**] approuvés **;**

3. Données, processus et supports

Délimiter et décrire le périmètre de manière détaillée en précisant :

- les **données** personnelles concernées, leurs **destinataires** et **durées de conservation ;**
- une description des **processus** et des **supports** de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement)

VII. ÉTUDE DES PRINCIPES FONDAMENTAUX

7.1. Objectif

- bâtir le dispositif de conformité aux principes de protection de la vie privée.

7.2. Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

Expliciter et justifier les choix effectués pour respecter les exigences suivantes :

- **Finalité(s)[Art. 383.3 du CDN]** : déterminée, explicite et légitime ;
- **Fondement** : licéité du traitement, interdiction du détournement de finalité[**383.2 du CDN**];
- **Minimisation des données [Art. 424 du CDN]** : adéquates, pertinentes et limitées ;
- **Qualité des données** : exactes et tenues à jour [**Art. 383.5**];
- Durées de conservation [Art. 433 du CDN] : limitées sauf accord de l'Autorité;

Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément aux dispositions du livre Vème du code du numérique. Le cas échéant, revoir leur description ou proposer des mesures complémentaires

VII. ÉTUDE DES PRINCIPES FONDAMENTAUX

7.3. Évaluation des mesures protectrices des droits des personnes des personnes concernées

- Identifier ou déterminer et décrire, les **mesures retenues** (existantes ou prévues) **pour respecter les exigences tout en expliquant** comment il est prévu de les mettre en œuvre suivantes:
  - **Information**[**Art. 415,416, 403 et 384 du CND**] des personnes concernées [traitement loyal et transparent] ;
  - **Recueil du consentement**[**Art. 389 du CND**] le cas échéant : exprès, démontrable, retirable ;
  - Exercice des **droits d'accès et à la portabilité** [**Art. 415,416, 403 et 384 du CND**]
- Exercice des **droits de rectification et de suppression**[Article.[**Art.441 du CND**], **et d'effacement** [**Art. 33, 437.6 du CND**];
- **E**xercice des **droits de limitation du traitement** [**Art. 437.6 du CND**] **et d'opposition** [**Art. 440 du CND**];
- **Sous-traitance** [Art. 426 alinéas 4 et 5 du CND] : identifiée et contractualisée[Art. 441 du CND];
- **Transferts** [Art. 391 et 392 du CND] : respect des obligations en matière de transfert de données en dehors de la CEDEAO/UEMOA

VII. ÉTUDE DES PRINCIPES FONDAMENTAUX

7.4. Étude des risques liés à la sécurité des données

1. Risque sur la vie privée

- Un risque est un **« Danger éventuel, plus ou moins prévisible, inhérent à une situation ou à une activité »** en d'autres termes **« Éventualité d'un événement futur, incertain ou d'un terme indéterminé, ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage »**. (ex. : accès non autorisé aux données personnelles)

On peut citer [non-exhaustive] :

- la discrimination ;
- le vol ou l'usurpation d'identité ;
- E-Réputation;
- la perte de confidentialité de données protégées par le secret professionnel ou lorsque le traitement concerne des données personnelles sensibles ;
- un accès illégitime aux données personnelles ;
- violation de l'intégrité des données personnelles ;
- erreurs humaines ;

VII. ÉTUDE DES PRINCIPES FONDAMENTAUX

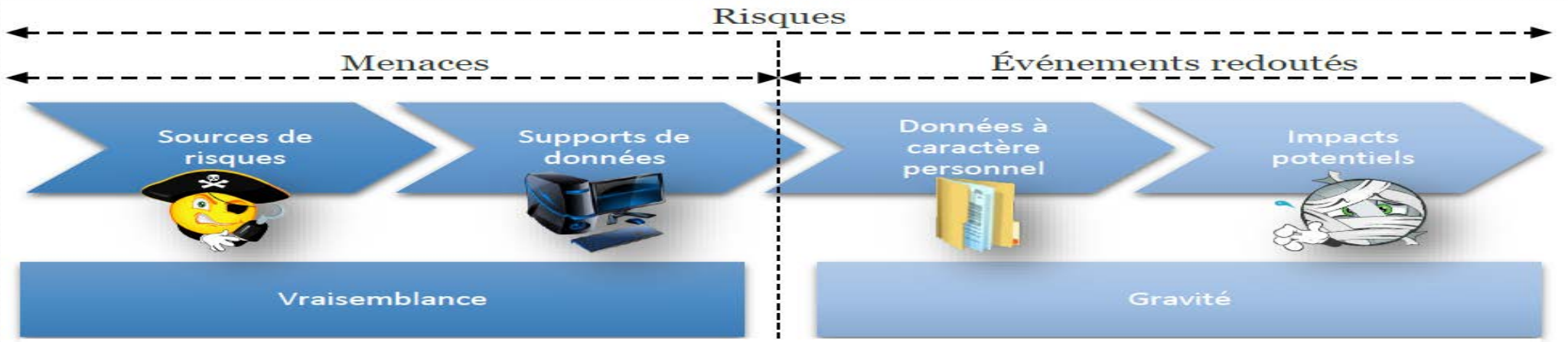
Autrement dit, la donnée personnelle, si elle n'est pas confinée et sécurisée, peut être une matière dangereuse.

Le niveau d'un risque est estimé en termes de **gravité et de vraisemblance :**

la **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels ;

la **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter

Le schéma suivant synthétise l'ensemble des notions présentées



VIII. ÉVALUATION DES MESURES EXISTANTES OU PREVUES

8.1. Objectif

Avoir une bonne connaissance des mesures contribuant à la sécurité.

8.2. Evaluation des mesures

- identifier ou de déterminer les **mesures existantes ou prévues** (déjà engagées), qui peuvent être de trois natures différentes :
  - **mesures portant spécifiquement sur les données du traitement** : chiffrement, anonymisation, pseudonymisation, cloisonnement, contrôle d'accès, traçabilité, etc. ;
  - **mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** : sécurité de l'exploitation, sauvegardes, sécurité des matériels, etc. ;
  - Mesures organisationnelles (gouvernance) : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, etc ;
  - Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité ;
  - Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

IX APPRECIATION DES RISQUES : LES ATTEINTES POTENTIELLES A LA VIE PRIVEE

9.1. Objectif

- Avoir une bonne compréhension des causes et conséquences des risques

9.2. Appréciation des risques

Pour chaque risque redouté :

- identifier les **menaces** sur les supports des données qui pourraient mener à cet événement redouté et les **sources de risques** qui pourraient en être à l'origine ;
- déterminer les **impacts** potentiels sur la vie privée des personnes concernées s'ils survenaient ;
- Estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
- Estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier;
- Déterminer si les risques ainsi identifiés peuvent être jugés acceptables compte tenu des mesures existantes ou prévues ;
- Dans la négative, proposer des mesures complémentaires et ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.

X. VALIDATION DU PIA

10.1. Objectif :

- Décider d'accepter ou non le PIA au regard des résultats de l'étude

10.2. Préparation des éléments utiles à la validation

- Consolider et mettre en forme les résultats de l'étude :
- Présenter une visuelle des **mesures choisies pour respecter les principes fondamentaux**, en fonction de leur conformité aux dispositions du Code du numérique (ex : à améliorer, ou jugé comme conforme) ;
- Représenter une visuelle des **mesures choisies pour contribuer à la sécurité des données**, en fonction de leur conformité aux bonnes pratiques de sécurité (ex : à améliorer, ou jugé comme conforme) ;
- Elaborer une cartographie visuelle des **risques résiduels** en fonction de leur gravité et vraisemblance ;
- Elaborer un **plan d'action** à partir des mesures complémentaires identifiées lors des étapes précédentes :
- pour chaque mesure, déterminer au moins le responsable de sa mise en oeuvre, son coût (financier et/ou en termes de charge) et son échéance prévisionnelle;

X. VALIDATION DU PIA

- **Formaliser la prise en compte des parties prenantes :**
  - **le conseil de la personne en charge des aspects liés au système d'information;**
  - **l'avis des personnes concernées ou de leurs représentants.**

10.2. Validation formelle

Décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes.

Le PIA peut ainsi être :

- validé ;
- à améliorer (expliquer en quoi) ;
- refusé (ainsi que le traitement considéré).

Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé

XI. **CARTOGRAPHIE DES TRAITEMENTS**

Après la désignation du responsable de la mise en conformité de l'organisation et celle des personnes impliquées dans le processus , l'opération de mise en conformité débute avec l'implication du DPO s'il est nommé, par un **audit des données personnelles et par la cartographie des traitements de données personnelles.** Bien maîtriser la méthodologie de cette étape est importante pour la suite du projet de mise en conformité.

elle permettra de :

- De comprendre les flux de données au niveau de l'organisation ;
- De constituer la documentation légale obligatoire (registre des traitements, clauses contractuelles, demande de consentement, exercice des droits, etc…) ;
- De prioriser le plan de mise en conformité et piloter sa mise en œuvre.

- Mais concrètement, comment faire la cartographie des traitements de données à caractère personnel de l'organisation ?

XI. **CARTOGRAPHIE DES TRAITEMENTS**

1. Par où commencer ?

- Définir avec toutes les parties prenantes les éléments nécessaires à l'initialisation et au bon déroulement du projet de cartographie. L'objectif et l'enjeu de ce projet sont de constituer une documentation interne complète des traitements de données personnelles et s'assurer de leur conformité aux obligations légales;

- Formaliser le **périmètre à cartographier** pour s'assurer que toutes les parties prenantes partagent la même vision puis, définir la **cartographie cible;**

- **Le périmètre à cartographier doit comprendre :**

  - **Les acteurs (internes ou externes) qui traitent ces données** : identifier les prestataires sous-traitants afin d'actualiser par la suite les clauses de confidentialité ;
  - **Les flux en indiquant l'origine et la destination des données,** afin notamment d'identifier les éventuels transferts de données hors de la CEDEAO/UEMOA.

XI. **CARTOGRAPHIE DES TRAITEMENTS**

2. Quel modèle de cartographie des traitements de vos données choisir ?

- Regrouper et analyser dans un premier temps les éléments de cartographie existants. En pratique, il faut :
  - **Recueillir et analyser l'ensemble des documents relatifs à la protection des données par rapport au Code du numérique,** aux éventuelles normes spécifiques, l'inventaire des ressources et des actifs ;
  - Identifier les outils de cartographie déjà en place ;
  - Identifier les processus existants concernant l'alimentation et la mise à jour des données personnelles ;
  - Identifier les difficultés rencontrées dans la constitution et l'utilisation des cartographies précédentes;
  - Définir le modèle de cartographie décrivant l'ensemble des entités ou systèmes qui gravitent autour des traitements de données et pour avoir d'une **vision claire de l'écosystème** sans se limiter à l'étude individuelle de chaque entité.

XI. **CARTOGRAPHIE DES TRAITEMENTS**

3. Quels outils de cartographie des traitements des données choisir ?

Le choix d'outils dépend du niveau de maturité visé et du contexte mais ils doivent à minima satisfaire les besoins suivants :

- Constituer l'inventaire des traitements des données et des finalités de traitement (registre des traitements) ;
- Réaliser des vues et représenter les liens entre elles ;
- Mettre en œuvre et contrôler le processus de maintien à jour de la cartographie.

Les outils de modélisation du système d'information et des vues spécifiquement construits pour rendre compte des traitements des données permettent, en plus de la réalisation de schémas et d'inventaires, de simplifier les actions de mise à jour et de partage des informations. Pour ces raisons, il est conseiller d'utiliser des logiciels dédiés à la cartographie souvent plus commode et efficace. Néanmoins, les organisations qui n'ont pas une grande maturité sur ces sujets, peuvent utiliser le modèle de registre de l'Autorité de Protection des données personnelles (APDP) et réaliser manuellement des schémas du système d'information et des vues des flux entrants et sortants de l'organisation en complément d'information.

XI. **CARTOGRAPHIE DES TRAITEMENTS**

4. Comment construire une cartographie des traitements des données ?

Au cas où l'organisation dispose déjà d'une cartographie **l'objectif sera de compléter l'inventaire et les différentes vues de manière incrémentale (enrichissement par de nouvelles vues) et itérative (affinement des vues déjà constituées).**

Pour les organisations qui n'en disposeraient pas, il faudra les créer sur la base :

- Des entretiens ciblés;
- Des outils de collecte automatique tels que les outils de gestion de parc ou les logiciels de supervision ;
- Des données extraites depuis des applications spécifiques (base de données, tableaux de bord, etc.) ;
- Des documents internes liés à la protection des données, à la collecte, au traitement, au stockage et à la suppression des données.

XI. **CARTOGRAPHIE DES TRAITEMENTS**

A cette étape un premier résultat aura été obtenu si :

- Tous les responsables de services et des entités qui traitent des données personnelles ont été rencontrés;
  - Toute la liste des traitements par finalité principale (et non par outil ou applicatif utilisé) et des types de données traitées a été effectuée ;
  - Tous les sous-traitants qui interviennent sur chaque traitement ont été identifiés et enregistrés ;
  - Les destinataires des données personnelles dans le cadre de transfert et leurs lieux de résidence sont enregistrés ;
  - Les lieux de stockage des données personnelles sont identifiés et pris en compte ;
  - Les durées de conservation des données personnelles sont consignées

XI. **CARTOGRAPHIE DES TRAITEMENTS**

Une fois l'inventaire terminé il faut construire les vues de la cartographie. En pratique, tous ces travaux peuvent être réalisés en parallèle.

Que les vues soient générées par un outil dédié ou manuellement, elles devront comporter un titre, un numéro de version et une légende.

Il est important de considérer chaque schéma comme un extrait à un instant T et non comme définitif ou final. La cartographie doit s'inscrire dans une démarche d'amélioration continue à la fois incrémentale et itérative.

5. Et après ?

Une fois cette cartographie terminée l'organisation dispose de l'ensemble des informations nécessaires pour **construire ou compléter le registre des traitements qui permettra d'identifier les actions à mener pour se conformer aux obligations actuelles et à venir de la loi.** Ces actions doivent être priorisées au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

1. Introduction

L'objectif principal de ce document est de regrouper dans un format concis, transparent, compréhensible et aisément accessible des informations concernant les traitements de données mis en œuvre pour comprendre dans quelles conditions les données sont traitées.

2. Une collecte loyale et transparente de vos données

- Dans un souci de loyauté et de transparence, l'organisation prendra soin d'informer les personnes concernées par chaque traitement qu'il met en œuvre par des mentions d'information.
- Ces données sont collectées loyalement. Aucune collecte n'est effectuée à l'insu des personnes et sans qu'elles en soient informées.

3. Une utilisation légitime et proportionnée des données

Lorsque l'organisation est amenée à traiter des données, il le fait pour des finalités spécifiques : chaque traitement de données mis en œuvre poursuit une finalité légitime, déterminée et explicite qui doit être précisée.

Pour chacun des traitements mis en œuvre, l'organisation devra s'engager à ne collecter et n'exploiter que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

- L'organisation doit veiller à ce que les données soient mises à jour. Elle doit mettre en œuvre des procédures permettant l'effacement ou la rectification des données inexactes.

4. Les données à caractère personnel en traitement

Dans le cadre des traitements de données à caractère personnel dont les finalités seront présentées, l'organisation doit présenter la liste des catégories de données personnelles traitées. Par exemple :

- Données d'identification des personnes concernées telles que : la civilité, les nom et prénoms, les coordonnées électroniques, téléphoniques et postales ;
- Des données relatives à la situation professionnelle de la personne concernée telles que la profession ou encore les coordonnées professionnelles ;
- Des données d'ordre économique et financier ;
- Enregistrement des visioconférences et webinaires organisés par le l'organisation (vidéo, contenu, message, tableau de bord et rapports) ;

- Etc….

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

5. Les bases juridiques et les finalités de traitements de données

- En exemple ci-dessous le remplissage du tableau des données traitées, des finalités et bases juridiques au tit chaque traitement

Données traitées	Finalités	Base juridique
Gestion de la production et suivi des dossiers clients	Constituer une base de données des prospects et des clients	Nécessaires à l'exécution d'un contrat ou à l'exécution des mesures précontractuelles prises à la demande des clients
Gestion des prestataires et partenaires	Constituer une base de données des prestataires et partenaires	Nécessaires à l'exécution d'un contrat ou à l'exécution des mesures précontractuelles prises à la demande des clients
Etc…		

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

6. Les destinataires des données

L'organisation précisera nommément les destinataires des données qui peuvent être:

- La liste des membres habilités de l'organisation ;
- La liste des personnes tierces habilitées à intervenir pour les besoins des missions confiées à l'organisation ;
- Les autorités ou juridictions compétentes ;

L'organisation veillera à ce que seules les personnes habilitées puissent avoir accès aux données. L'organisation précisera la politique d'habilitation c'est dire à qui les données sont transmises et ceux qui y ont accès.

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

7. Les transferts des données

L'organisation est susceptible de transférer des données personnelles en dehors de la CEDEAO/UEMOA dans le cadre de ses activités.

Il devra préciser :

- Les mesures de sécurisation, en veillant par exemple à la conclusion des clauses types définies par la loi ;Les outils de messagerie, de gestion des agendas, visioconférence, webinaire, etc… ;
- Les lieux d'hébergement des applications ;
- Les destinataires habilités ;
- Les conventions de flux transfrontières sur la base des clauses contractuelles types conclues ;
- Les autorisations de l'Autorité de protection ;

Etc…

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

8. Les durées de conservation des données

- L'organisation précisera la durée de conservation des données personnelles en référence au code du numérique et proportionnées aux finalités pour lesquelles elles ont été collectées. Le tableau qui suit peut-être renseigné.
- Plus précisément, nous organisons notre politique de conservation des données de la manière suivante :

Liste des données	Finalités	Durée de conservation	Dispositions juridiques

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

9. La sécurité des données personnelles

L'organisation doit décrire le système de sécurisation des données personnelles. Elle indiquera les mesures techniques et organisationnelles adaptées au degré de sensibilité des données personnelles, en vue d'assurer l'intégrité et la confidentialité des données et leur protection contre toute intrusion malveillante, toute perte, altération ou divulgation à des tiers non autorisés.

10. La sous-traitance

L'organisation précisera dans le document la liste de tous ses sous-traitants y compris les obligations légales et réglementaires des contrats définissant précisément les conditions et modalités de traitement des données personnelles par ces derniers, en conformité avec la réglementation sur la protection des données personnelles.

11.Cookies

L'organisation précisera sa politique des cookies qui doit être définie.

XII. POLITIQUE DE PROTECTION DES DONNES PERSONNELLEs

12. Les droits des personnes concernées

L'organisation devra être particulièrement soucieux du respect des droits des personnes dont les données personnelles sont en traitement qu'elle met en œuvre, pour garantir des traitements équitables et transparents compte tenu des circonstances particulières et du contexte dans lesquels les données personnelles sont traitées. A ce titre, elle précisera tous les droits des personnes concernées par le traitement en référence à la loi.

13. Révision document de politique

Préciser la mention de révision et des critères de révision

Merci pour votre aimable attention

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/

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