COMMENT STRUCTURER UN PROGRAMME DE MISE EN CONFORMITE

APDP, 07 au 09 juin 2022

By 360 conseils S.A.S

SOMMAIRE

INTRODUCTION

Dans le monde informatique notamment, la conformité est une nouveauté. Plus singulièrement, au nombre des bouleversements apportés par le CDN, la notion de conformité n'a pas vite émergé. Elle occupe pourtant une place de choix et il faut croire qu'elle deviendra une réalité de plus en plus évidente au cours des deux, trois prochaines années.

La conformité, c'est le fait de se conformer à une situation de fait, une règle, un texte juridique. En l'espèce, la conformité, c'est principalement le fait de s'aligner sur les exigences du Code du numérique. Mais également aux instruments juridiques applicatifs auxquels il renvoie. Certains de ces instruments seront du fait de l'Autorité (normes, référentiels, certifications etc.) tandis que d'autres proviendront des acteurs eux-mêmes (codes de conduite, Binding Corporate Rules-BCR etc.).

Ensemble avec le CDN, ces différents instruments devraient renseigner principalement sur les démarches utiles qui conduiront vers la conformité. Le Code du numérique par exemple a mis en place une batterie d'obligations à la charge des entreprises tant vis-à-vis de l'Autorité que vis-à-vis des personnes, défini les divers régimes de responsabilités, créé de nouveaux métiers. Le respect de ces ordonnancements devra alors permettre d'être conforme.

I-

L'OPPORTUNITE DES CODES DE CONDUITE

I- L'OPPORTUNITE DES CODES DE CONDUITE

Dans la pratique internationale, le code de conduite est perçu comme un outil de conformité sectoriel qui permet de répondre aux besoins opérationnels des professionnels concernés dans leurs démarches de mise en conformité.

Le code de conduite s'élabore à partir des exigences contenues dans la règlementation nationale et résulte d'une double démarche volontaire :

La décision par l'organisation représentative du secteur d'élaborer un code et

L'adhésion des professionnels concernés.

C'est un outil à vocation pratique qui répond aux besoins des professionnels du secteur concerné, notamment des micros, petites et moyennes entreprises afin de les aider à appliquer les dispositions légales.

Il doit être rédigé de façon claire et compréhensible pour être applicable par des professionnels qui ne sont pas nécessairement des experts en matière de protection des données.

I- L'OPPORTUNITE DES CODES DE CONDUITE

Un code de conduite est un outil juridiquement contraignant : il s'impose à ceux qui y adhèrent.

Il doit être mis en place par une organisation représentative d'un secteur d'activité.
Le code de conduite permet de :

Construire un socle commun de bonnes pratiques en matière de protection des données

Démontrer sa conformité aux exigences légales sur le périmètre du code de conduite ;

Harmoniser les pratiques d'un secteur ;

Répondre aux besoins des micros, petites et moyennes entreprises dans leur démarche de mise en conformité en leur fournissant un instrument simple et opérationnel.

I- L'OPPORTUNITE DES CODES DE CONDUITE

En présence de groupes d'entreprises, notamment d'entreprises multinationales, le code de conduite est décliné sous forme de règles contraignantes de conduite (Binding Corporate Rules - BCR) destiné à harmoniser les pratiques et à offrir des garanties suffisantes de protection des DCP en passant d'un Etat à un autre.

Il est fortement recommandé que les organismes traitants réfléchissent à la mise en place de codes de conduite afin de faciliter leurs démarches de mise en conformité.

CONTENU DU CODE DE CONDUITE

01 Introduction (objectifs, champ d'application, organismes membres, légitimité du porteur etc.)

02 Le champ d'application matériel (les traitements de données concernés) et territorial (l'État ou les États dans lequel ou lesquels il sera en vigueur) ;

03 L'autorité de contrôle compétente du Code

04 Modalités d'adhésion au code de conduite, le mécanisme de sortie du code, le processus de mise à jour des exigences du code, les critères de sélection de l'organisme de contrôle, etc.

05 L'organisme en charge du contrôle régulier de la bonne application du code de conduite par les adhérents ;

06 Résumé de la consultation des professionnels du secteur et si possible des personnes concernées

07 Le cadre juridique applicable

08 La langue du code de conduite

II-

COMMENT VOUS METTRE EN CONFORMITE ?

II-

COMMENT VOUS METTRE EN CONFORMITE ?

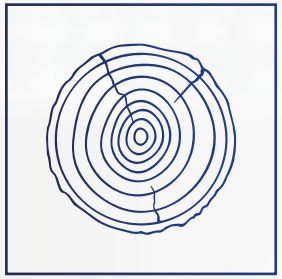
« Il n'existe pas LA démarche de conformité, mais des démarches que les échanges de bonnes pratiques entre professionnels et les échanges documentent et améliorent »

« La mise en conformité est un vaste chantier de construction de mesures organisationnelles et logicielles. »

Pour la construire, il faudra constituer au prime abord une équipe projet ou désigner un responsable projet.

A LE COMITE DE PILOTAGE DE PROJET

Le comité de pilotage (ou COPIL) a pour objectif d'assurer le bon fonctionnement du projet.



La transversalité du projet de conformité

La mise en conformité n'est pas nécessairement un projet technique, réservé aux informaticiens, ni juridique, réservé aux juristes etc.
La mise en conformité est surtout un projet transverse qui est appelé à mobiliser tous les acteurs de l'entreprise.

Le caractère politique du projet de mise en conformité

« Candidat cherche parrain »

Le DPO, un acteur légalement institué et indispensable

« Pas de navire sans capitaine » : il coordonne l'activité de mise et maintien en conformité
Le profil requiert autonomie, indépendance et impartialité, le DPO devra être « un élu ingrat ».
Il peut être membre de l'entreprise ou agir en qualité de prestataire externe (cabinet de consulting…).

Enfin, le DPO n'est pas responsable de la conformité au CDN.

COMPOSITION TYPE DU COPIL

Le sponsor :

Arbitre et soutien du directeur de projet
Bailleur de moyens

Le directeur de projet :

Guide
Grâce à sa hauteur de vue, le directeur de projet fluidifie la compréhension du projet par les équipes techniques, commerciales et organisationnelles.

Les chefs de projet techniques et fonctionnels

La Direction des Systèmes d'Information intervient sur les aspects techniques, en particulier dans la phase de diagnostic des données mais également sur l'aspect sécurité

Les responsables RH, marketing, commercial, technique ou encore juridique sont amenés à donner leur éclairage sur les enjeux liés à leur champ de compétences respectifs au fil du déroulement du projet

Cette sélection est importante puisqu'elle a une influence sur les prises de décisions.

Dans une matière à la croisée de presque tous les secteurs d'intervention de l'entreprise, certaines exigences ne sont pas nouvelles et sont peut-être déjà en application. Pour cela, il est important de procéder à une évaluation de la situation de l'entreprise vis-à-vis du CDN à travers une revue initiale de conformité.

B LA REVUE INITIALE DE CONFORMITE

Il faut commencer par évaluer son positionnement vis-à-vis des exigences du CDN. Cette étape commence par un recensement des pratiques internes pour se terminer avec la définition d'un plan d'action d'où seront priorisées lesquelles menées.

01 CARTOGRAPHIE DES DONNEES

L'idée, comme sa mise en œuvre est simple : relever le plus exhaustivement possible les traitements mis en œuvre.

La cartographie des traitements de données personnelles consiste à identifier et à répertorier tous les traitements au sein de l'organisme.

II- COMMENT VOUS METTRE EN CONFORMITE ?

Pour chaque traitement de données personnelles, il faut se poser les questions ci-après :

QUI ?

- Inscrire dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données
- Identifier les responsables des services opérationnels traitant les données au sein de votre organisme
- Etablir la liste des sous-traitants

QUOI ?

- Identifier les catégories de données traitées
- Identifier les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple : les données relatives à la santé ou les infractions)

POURQUOI ?

Indiquer la ou les finalités pour lesquelles vous collectez ou traitez ces données (par exemple : gestion de la relation commerciale, gestion RH...)

OU ?

Déterminer le lieu où les données sont hébergées

Indiquer vers quels pays les données sont éventuellement transférées

JUSQU'À QUAND ?

Indiquer, pour chaque catégorie de données, combien de temps vous les conservez

COMMENT ?

Préciser les mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées

Au cours de cette étape, il n'est pas superflu collecter les documents existants relatifs au SI et à la SSI et de commencer à constituer la liste des documents obligatoires/nécessaires.

02 PRIORISATION DES ACTIONS

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de l'organisme, il faut, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir.

La priorisation tiendra compte des écarts de conformité en l'état actuel. Mais elle doit également être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées.

Certaines considérations comme la minimisation des données, la détermination de la base légale, la rédaction des mentions d'informations etc. seront faciles à mettre en œuvre et vous permettront de progresser rapidement.

Par contre, si vous traitez certains types de données, une ou des analyses d'impact s'imposera(ont) et influencerons votre progression.

C

L'ANALYSE D'IMPACT RELATIF A LA PROTECTION DES DONNEES

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.

« 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** » (article 428 CDN), vous devez réaliser une AIPD.

De même, le recours à une nouvelle technologie implique presque toujours un risque d'atteinte au respect des droits et libertés individuelles du patient.

C

CRITERES DE DECLENCHEMENT DE L'AIPD

Un cadre général de déclenchement de l'analyse est mis en place par le CDN. Mais également par la Convention 108+ dont nous sommes observateurs. Concrètement, en l'état législatif actuel, il faut réaliser une AIPD dans les situations suivantes :

- soit le traitement envisagé figure dans la liste des types d'opérations de traitement (à éditer) pour lesquelles l'APDP a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données ;
- Soit le traitement remplit au moins deux des neuf critères issus des lignes directrices du Groupe de Travail sur l'article 29 du RGPD dont :

Evaluation/notation (scoring) (y compris le profilage)
Par exemple, un traitement d'analyse des usages d'internautes afin de créer des profils comportementaux ou marketing.

C

Décision automatique avec effet légal ou similaire

Par exemple, le traitement conduit à une discrimination ou à l'exclusion. Si le traitement ne conduit que très peu d'effet, il ne sera pas concerné.

Surveillance systématique

Par exemple, la surveillance systématique sur les réseaux ou dans l'espace public.

Collecte de données sensibles ou données à caractère hautement personnel

Origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, données concernant la vie ou l'orientation sexuelle, données relatives à des communications électroniques, données de localisation, données relatives à des condamnations pénales, infractions ou mesures de sûreté.

C

Collecte de données personnelles à large échelle

Il faut prendre en compte le nombre de personnes concernées, le volume de données ou le spectre des données, la durée ou la permanence du traitement et l'étendue géographique du traitement.

Croisement de données

Autrement dit, à quel traitement la personne peut-elle s'attendre dans le contexte de la collecte des données ? Plus il sera inattendu ou surprenant, plus il dépassera les attentes raisonnables.

Personnes vulnérables (patients, personnes âgées, enfants, etc.)

Par exemple de données de patients, personnes âgées, enfant, demandeurs d'asile etc. Dans une certaine mesure, il peut s'agir de données relatives à des employés au regard du lien de subordination avec l'employeur.

II-

COMMENT VOUS METTRE EN CONFORMITE ?

Usage innovant (utilisation d'une nouvelle technologie)

Par exemple, les applications de l'internet des objets ou la combinaison d'empreintes digitales et de reconnaissance faciale pour faire du contrôle d'accès.

Exclusion du bénéfice d'un droit/contrat

Par exemple, un outil de scoring dans le cadre d'un prêt bancaire.

Les transferts de données hors de la CEDEAO

Une AIPD n'est pas requise si le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis, ou nécessaire à l'exercice d'une mission de service public confié au responsable de traitement et qu'une AIPD a été réalisée par l'autorité publique.

D GOUVERNER LA SECURITE DES DCP

La gouvernance interne devrait permettre de mettre en place des procédures qui garantissent la protection des données à tout instant.
Pour atteindre cet objectif, il faudra :

Prendre en compte de la protection des données personnelles dès la conception d'une application ou d'un traitement ;

Sensibiliser et organiser la remontée d'informations en construisant notamment un plan de formation et de communication auprès de vos collaborateurs ;

Constituer un dossier de conformité pour respecter votre obligation de redevabilité (accountability).

D

01 PRIVACY BY DESIGN ET BY DEFAULT

Le Privacy by Design est une évolution des PETs.

Les PETs sont à l'origine du principe de « minimisation des données », c'est sur la base de ce principe que s'est développé ce concept de Privacy by Design.

La démarche permet de réaliser des projets informatiques de sorte à protéger les données à caractère personnel des personnes concernées par lesdits projets.

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 inopérantes in fine.

Le code du numérique consacre la notion en droit béninois notamment en son article 424. Mais au-delà de cet article nominatif, la notion est traitée à travers une bonne partie du code de manière implicite.

7

LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

II-

COMMENT VOUS METTRE EN CONFORMITE ?

7 LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

01 A priori & pas a posteriori (Article 424 al 1 CDN)

Il faut anticiper et empêcher les événements envahissants dans la vie privée avant qu'ils ne se produisent.

Les mesures proactives doivent être préférées aux mesures réactives

Les mesures préventives doivent être préférées aux mesures correctives

L'objectif alors visé ici est d'anticiper les incidents à la vie privée avant leur survenance. La protection intégrée de la vie privée doit intervenir avant le fait, pas après.

LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

02 Confidentialité comme paramètre par défaut (Article 424 al 2 et 425 CDN)

- Si un individu ne fait rien, sa vie privée reste intacte.
- Aucune action n'est requise de la part de l'individu pour protéger sa vie privée-celle-ci est intégrée au système spontanément, par défaut.
- Le système conçu doit défendre la vie privée de l’utilisateur à son insu

LES 7 PRINCIPES DU PRIVACY
BY DESIGN AND BY DEFAULT

03 Confidentialité intégrée à la conception (Article 424 CDN)

La protection intégrée de la vie privée est intégrée à la conception et à l'architecture des systèmes informatiques et des pratiques de l'entreprise. Ce n'est pas un ajout, après coup.

Il en résulte que la confidentialité devient un élément essentiel de la fonctionnalité principale fournie.

7 LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

04 Paradigme à somme positive et non à somme nulle

La prise en compte de la vie privée ne doit pas empêcher la mise en œuvre d'autres fonctionnalités.

Il est possible de réaliser plusieurs objectifs à la fois sans les compromettre.

Les fonctionnalités doivent être fournies intégralement selon un paradigme à somme positive et non à somme nulle

Implique une analyse d'impact -- Article 428, 429 CDN

7 LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

04 Paradigme à somme positive et non à somme nulle

Quand la préservation de la vie privée s'oppose à la sécurité, c'est une hérésie

Quand la sécurité de la vie privée est garantie au détriment d'une fonctionnalité intégrale, c'est un compromis inutile

Le défi imposé par la loi est celui de réussir à garantir la sécurité de la vie privée tout en offrant une fonctionnalité intégrale et en faisant une bonne affaire.

Ainsi d'autres aspects non moins importants peuvent prendre le pas sur la protection de la vie privée aux termes d'un audit d'impact.

7 LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

04 Paradigme à somme positive et non à somme nulle

L'objectif visée ici est que le souci de la protection de la vie privée ne doit pas mener à faire perdre au projet, sa substance.

05 La sécurité de bout en bout et pendant tout le cycle de vie du produit (Articles 426, 433,434, 435 CDN)

Des mesures de sécurité essentielles à la protection de la vie privée sont mises en œuvre du début jusqu'à la fin.

LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

05 La sécurité de bout en bout et pendant tout le cycle de vie du produit (Articles 426, 433,434, 435 CDN)

- Cela permet d'assurer la conservation sécurisée des données, puis leur destruction sécurisée à la fin de leur période de conservation.
- Il est question de préserver la sécurité des données personnelles : au moment de leur recueil, pendant leur traitement et à la fin de leur traitement.
- Pseudonymisation : chiffrement des données collectées avant leurs transferts
- Hautes mesures sécuritaires : confidentialité, intégrité, disponibilité et résilience

LES 7 PRINCIPES DU PRIVACY
BY DESIGN AND BY DEFAULT

05

La sécurité de bout en bout et pendant tout le cycle de vie du produit (Articles 426, 433,434, 435 CDN)

- Plan de continuité d'activités : assurer la continuité du service
- Evaluation régulière du système de sécurité
- Assurance : souscription si possible d'une police d'assurance adéquate

7 LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

06 Assurer la visibilité et la transparence (Article 418-423-415-416-437-443-410 CDN)

Les éléments et le fonctionnement du système demeurent visibles et transparents, tant pour les utilisateurs que pour les fournisseurs.

La vérification permet d'établir un climat de confiance

LES 7 PRINCIPES DU PRIVACY BY DESIGN AND BY DEFAULT

07 Une confidentialité centrée sur les besoins des utilisateurs

Minimisation : les finalités poursuivies doivent correspondre aux informations requises.

Evitez les demandes voyeuristes et encombrantes.

Il s'agit d'offrir aux clients la garantie d'un traitement des données qui soit à la fois parfaitement sûr et qui corresponde exactement à leur besoin, sans collecter plus de données que nécessaire.

D

02 LES CHANTIERS DE IN(FORMATION)

01 Communication du top management auprès du personnel pour le préparer à ces changements à venir.

02 Le personnel doit être également sensibilisé à la protection des données à caractère et le RT doit pouvoir le démontrer.

03 Enfin, les diverses procédures mises en place doivent être vulgarisées auprès du personnel pour s'assurer qu'elles recevront l'application escomptée.

03 LE DOSSIER DE CONFORMITÉ

Démontrer sa conformité, c'est produire une documentation exhaustive et détaillée, décrivant l'ensemble des procédures et des bonnes pratiques appliquées par l'organisme en matière de données personnelles.

LES FONDAMENTAUX DE LA CONFORMITÉ :

- Code d'éthique sur les principes fondamentaux appliqués par l'organisme
- Documentation relative à la nomination du DPO et ses relais locaux
- Cartographie des traitements et schémas des flux de données
- Registre des traitements
- Fiches par traitement (précisions et justifications détaillées des choix et prises de position effectuées)

TRANSPARENCE ET INFORMATION DES PERSONNES :

- Procédure sur la gestion des demandes de droits d'accès CDN par les salariés (suppression, opposition, portabilité, etc.)
- Procédure sur la gestion des demandes de droits d'accès par les clients
- Politiques de confidentialité interne destinée aux salariés de l'organisme
- Formulaires de consentement
- Modalités de gestion des preuves des recueils de consentements (traçabilité)
- Formulaires types permettant l'exercice des droits par les salariés et clients
- Traçabilité des traitements effectués en réponse aux demandes d'exercice des droits

SÉCURITÉ, INTÉGRITÉ ET CONFIDENTIALITÉ :

- Politique de Sécurité des Systèmes d'Informations (PSSI)
- Procédure sur les durées de conservation des données, l'archivage et la suppression
- Procédure sur la gestion et la notification des violations de données (data breach)
- Procédure sur la gestion et la conduite des analyses d'impact
- Procédure d'anonymisation/de pseudonymisation des données
- Procédure sur la gestion des projets impliquant les principes de privacy by design/ by default
- Codes de conduite par métier sur les conditions de traitement des données personnelles (DSI, RH, marketing, innovation)

SÉCURITÉ, INTÉGRITÉ ET CONFIDENTIALITÉ :

- Charte informatique
- Règlement intérieur
- Rapports des tests d'intrusion et plans d'actions de régularisation
- Rapports des analyses d'impact effectuées sur les traitements à risque
- Traçabilité des data breach et conditions de traitement des incidents rencontrés
- PCA - PRA
- Support de sensibilisation/formation CDN des salariés, feuilles de présence et thèmes abordés

ASPECTS CONTRACTUELS :

- Politique d'éthique du choix des fournisseurs et partenaires (sous-traitants)
- Liste exhaustive des sous-traitants, localisation et périmètre d'activité
- Procédure sur le transfert des données personnelles hors CEDEAO
- Convention intragroupe
- Contrats sous-traitants / avenants
- Contrat de travail des salariés (RH, DSI, marketing, etc.) traitant les données (clause sur obligation de confidentialité spécifique)

CONTRÔLE ET AUDIT DE L'EFFICACITÉ DES MESURES DÉPLOYÉES :

- Politique d'audit interne (périodicité, périmètre contrôlé, plan d'audit, tests sur échantillons aléatoires)
- Politique d'audit des sous-traitants (périodicité, périmètre contrôlé, plan d'audit)
- Comptes rendus des audits internes et indépendants effectués
- Plans d'actions de régularisation
- Traçabilité des modifications et mises à jour apportées au dossier d'accountability

RELATIONS APDP :

- Déclarations de conformité, demandes d'autorisations, demandes d'avis
- Questions écrites posées à l'APDP et réponses obtenues

EN GUISE DE RÉSUMÉ

L'APDP A ÉDITÉ LES 10 RÈGLES D'OR POUR RÉUSSIR UNE MISE ET UN MAINTIEN EN CONFORMITÉ :

01 EVALUER ET IDENTIFIER LE TRAITEMENT DE DONNÉES

02 DÉTERMINER LES INTERVENANTS ET PRESTATAIRES

03 CONCEVOIR ET METTRE EN PLACE LES MESURES DE SÉCURITÉ

04 FAIRE LES FORMALITÉS PRÉALABLES

05 SENSIBILISER LES COLLABORATEURS

06 PROCÉDER AUX MENTIONS D'INFORMATIONS ET ACTUALISER LES CONSENTEMENTS

07 DÉSIGNER LE DPO

08 RESPECTER LES DROITS DES DPC

09 ASSURER LA SÉCURITÉ

10 PRÉSENTER LES RAPPORTS CONTRE CERTIFICAT DE CONFORMITÉ

Veuillez retrouver le présent slide : **https://apdp.bj/formation-secteur-public-2022/**

Merci

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/