ANALYSE D'IMPACT, AUDIT & GESTION DES RISQUES

Cotonou le 06 06 2023

Par Ambroise Dj. ZINSOU
Consultant formateur indépendant
Management Télécoms & TIC et Protection
des données personnelles et de la vie privée

SOMMAIRE

INTRODUCTION

Le présent thème vise à présenter la démarche pour mener une "analyse d'impact relative à la protection des données" en application des dispositions de l'article 428 du CDN, plus communément appelée Privacy Impact Assessment (PIA) et des audits des données personnelles à effectuer tout au long de la vie des traitements pour s'assurer que l'organisation respecte les exigences de la loi et minimise les risques liés à la protection des données.

Le fonctionnement itératif de cette démarche doit permettre de garantir une utilisation raisonnée et fiable de données à caractère personnel dans le cadre de leur traitement.

L'analyse d'impact et l'audit constituent de précieux instruments pour s'assurer de la conformité des activités de traitement des données personnelles d'un organisme public ou privé à la loi.

Ils sont obligatoires lorsque le traitement est “*susceptible d’engendrer un risque élevé pour les droits et libertés des personnes concernées*”.

Dans la pratique, il s’agit d’un audit approfondi, d’un traitement en particulier. Sa mise œuvre conduit à déterminer la nécessité ou non de mettre en place un certain nombre d’actions afin de réduire les risques sur la vie privée des personnes concernées.

ANALYSE D’IMPACT

Le PIA s'adresse aux responsables de traitements qui souhaitent justifier de leur démarche de conformité à la loi et les mesures qu'ils ont choisies (notion de responsabilité ou d'accountability en anglais ainsi qu'aux fournisseurs de produits qui souhaitent démontrer que leurs solutions sont conçues dans une logique de conception respectueuse de la vie privée [notion de Protection des données personnelles dès la conception et la protection des données par défaut], [art. 424 du CDN].

Il est utile à toutes les parties prenantes dans la création ou l'amélioration de traitements de données à caractère personnel ou de produits :

- les autorités décisionnaires, qui commanditent et valident la création de nouveaux traitements de données à caractère personnel ou produits;
- ii. les maîtrises d'ouvrage, qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;

iii. les maîtrises d'œuvre, qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les maîtrises d'ouvrage;

iv. les correspondants ou délégués à la protection des données, qui doivent accompagner les maîtrises d'ouvrage et les autorités décisionnaires dans la protection des données à caractère personnel;

v. les responsables de la sécurité des systèmes d'information, qui doivent accompagner les maîtrises d'ouvrage dans le domaine de la sécurité des systèmes d'information.

COMMENT MENER UN PIA ?

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

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

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

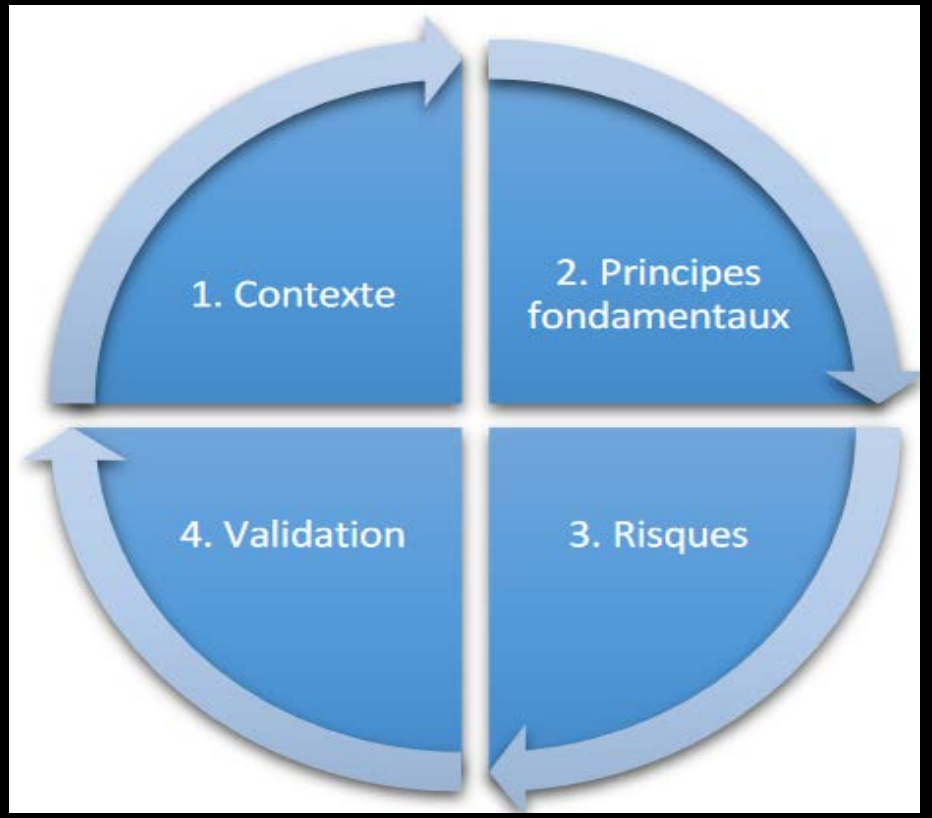
En résumé, pour mener un PIA, il convient de

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

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

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

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



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..

Étude du contexte

❑ **Objectif** : Avoir une vision claire des traitements de données personnelles considérés.

➢ Vue d'ensemble

Il s'agira de :

- Présenter le traitement considéré, sa nature, sa portée, son contexte, ses finalités et ses enjeux de manière synthétique;
- Identifier le responsable de traitement et les éventuels sous-traitants;
- Recenser les référentiels applicables au traitement, utiles ou à respecter, notamment les codes de conduite approuvés (cf. art. 413 du CDN) et des certifications en matière de protection des données s'il a lieu

➢ Données, processus et supports

Délimiter et décrire le périmètre de manière détaillée :

- 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).

Étude des principes fondamentaux

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

➢ **Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement**

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

- Finalité(s) : déterminée, explicite et légitime (cf. art. 383 du CDN);
- Fondement : licéité du traitement, interdiction du détournement de finalité (cf. art. 383 du CDN);

- Minimisation des données : adéquates, pertinentes et limitées (article 383.4 du CDN ;

- Qualité des données : exactes et tenues à jour (Article 383.5. du CDN) ;

- Durées de conservation : limitées (Article 383.6 du CDN).

  ➢Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément à la loi;

  ➢Dans le cas contraire, revoir leur description ou proposer des mesures complémentaires.

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 suivantes :

- Information des personnes concernées (traitement loyal et transparent, cf. art. 383.2 et 415 du CDN) ;
- Recueil du consentement, le cas échéant, démontrable, retirable (cf 389 du CDN);
- Exercice des droits d'accès et à la portabilité (cf. art. 415.9 & 438 & 445 du CDN);
- Exercice des droits de rectification et d'effacement (cf. art. 441 du CDN) ;

- Exercice des droits de limitation du traitement et d'opposition (cf. art. 440 du CDN) ;

- Sous-traitance : identifiée et contractualisée (Art. 386 du CDN);

- Transferts : respect des obligations en matière de transfert de données en dehors de l'espace UEMOA/CEDEAO (cf. art.391 du CDN).

➢ Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément à la loi.

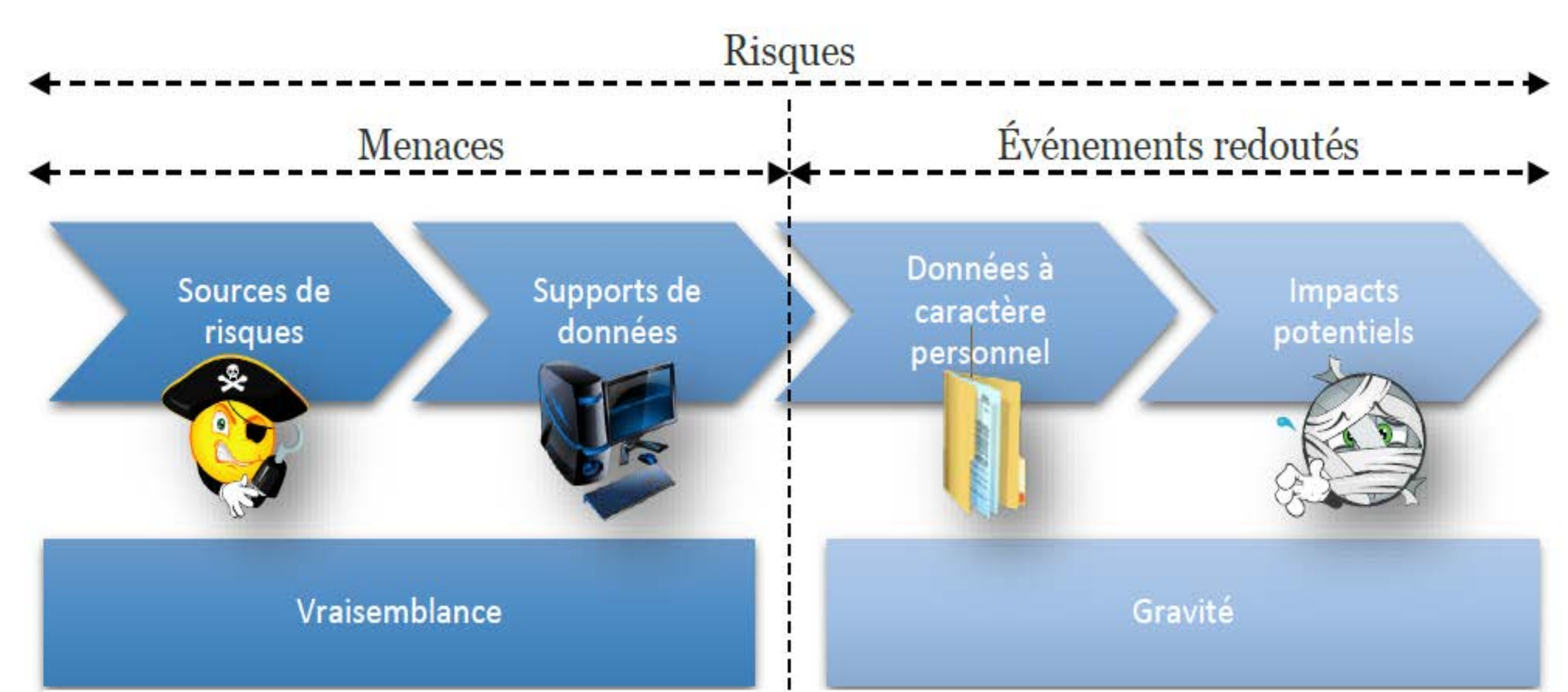
➢ Le cas échéant, revoir leur description ou proposer des mesures complémentaires

Étude des risques liés à la sécurité des données

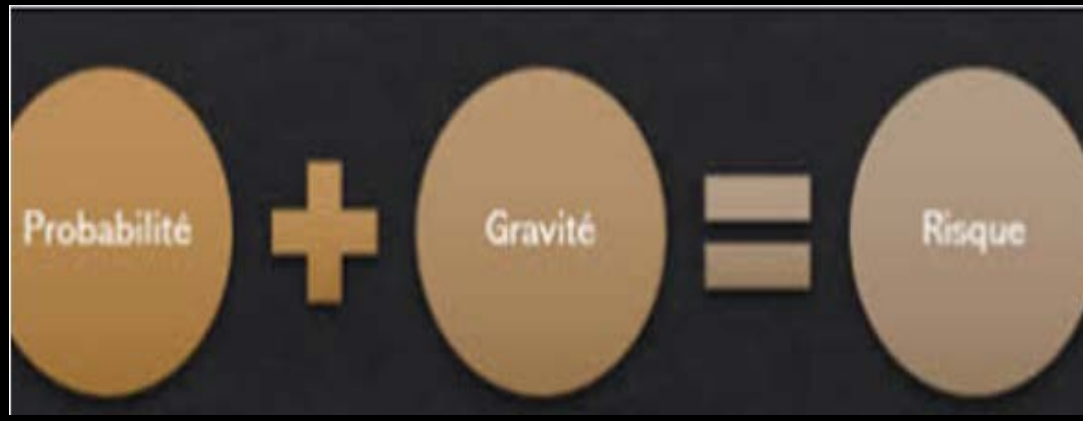
Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui pourraient permettre qu'il survienne. Plus précisément, il décrit :

- les sources de risques (ex. : un salarié soudoyé par un concurrent);
- les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données);
- les menaces (ex. : détournement par envoi de courriers électroniques) ;
- Les événements redoutés pouvant survenir (ex. : accès illégitime à des données) ;
- les risques sur les données à caractère personnel (ex. : fichier des clients);
- les impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels).

Le schéma suivant synthétise l'ensemble des notions présentées



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 ou la probabilité 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

❑Évaluation des mesures existantes ou prévues

❑Objectif : Obtenir une bonne connaissance des mesures contribuant à la sécurité

Identifier ou 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, cloisonnement, contrôle d'accès, traçabilité, etc. ;

- mesures générales de sécurité du système dans lequel le traitement est mis en oeuvre : 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.

- Appréciation des risques : les atteintes potentielles à la vie
- Objectif : obtenir une bonne compréhension des causes et conséquences des risques

Pour chaque événement redouté (un accès illégitime à des données, une modification non désirée de données et une disparition de données) :

- 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 ;
- 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 ;

- 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

Validation du PIA

❑Objectif : décider d'accepter ou non le PIA au regard des résultats de l'étude obtenus.

➢Consolider et mettre en forme les résultats de l'étude :

- Elaborer une représentation visuelle des mesures choisies pour respecter les principes fondamentaux, en fonction de leur conformité au livre V ème du CDN (ex : à améliorer, ou jugé comme conforme) ;
- élaborer une représentation 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) ;
- élaborer une cartographie visuelle des risques résiduels en fonction de leur gravité et vraisemblance ;

élaborer 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

- Formaliser la prise en compte des parties prenantes :
  - Le conseil de la personne en charge des aspects « organisationnels et techniques », si elle a été désignée (cf. art. 387 du CDN) ;
  - L'avis des personnes concernées ou de leurs représentants, le cas échéant (cf. art. 407 du CDN).

❑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.

AUDIT

L’audit, est un outil essentiel pour suivre la conformité l’organisation à la loi. Il est un moyen efficace de décrypter la manière de travailler et d’en tirer des recommandations pour améliorer la protection des données personnelles.

Le plus souvent l’audit vise un objectif précis :

Objectif 1 : Soit c’est un audit initial par rapport à la loi qui vise à faire un diagnostic factuel des écarts avec celle-ci (avec un plan d’action pour les corriger).

Objectif 2 : Soit c’est un audit de suivi de la démarche pour vérifier la continuité de l’implication de l’organisation et le respect des règles internes.

La mise en conformité avec le livre Vème du code du numérique est un processus continu, et les organisations doivent régulièrement effectuer ces audits pour s’assurer qu’elles respectent les règles.

En fonction des objectifs, un audit peut être effectué par une entreprise elle-même ou par une tierce partie (un consultant accrédité).

❑Préparation de l'audit

Avant de commencer l'audit des données personnelles , il est important de définir clairement les objectifs et les périmètres de l'audit. Cela inclut l'identification des parties prenantes internes et externes concernées, la définition des responsabilités et l'établissement d'un calendrier réaliste pour sa réalisation.

❑ Cartographie des données personnelles

L'une des étapes clés d'un audit réussi est la cartographie des données personnelles. Cela implique d'identifier, de catégoriser et de documenter les données personnelles que l'organisation traite, ainsi que les flux de données entre les différents systèmes et départements. La cartographie des données permet de mieux comprendre les risques liés à la protection des données et d'identifier les mesures à mettre en place pour assurer la conformité avec la loi.

❑Analyse des processus de traitement des données

Une fois la cartographie des données effectuée, il est important d'analyser les processus de traitement des données personnelles pour s'assurer qu'ils sont conformes aux exigences de la loi. Cela inclut la vérification de la légitimité des traitements, la gestion des consentements, l'application des principes de protection des données dès la conception et par défaut, et la mise en place des mesures de sécurité adéquates

❑Évaluation des risques

La loi requiert que les organisations évaluent les risques liés à leurs traitements de données personnelles et mettent en place des mesures pour les atténuer. L'évaluation des risques doit prendre en compte la probabilité et la gravité des impacts négatifs sur les droits des personnes concernées, ainsi que les mesures existantes pour minimiser ces risques.

❑Gestion des sous-traitants

La loi impose également des obligations aux organisations concernant la gestion de leurs sous-traitants. Il est donc essentiel d'évaluer la conformité des partenaires et de mettre en place des contrats de sous-traitance adéquats pour encadrer les traitements de données personnelles réalisés pour le compte de l'organisation

❑Mise en œuvre des mesures de protection des données

Sur la base des résultats de l'audit, il convient de mettre en œuvre les mesures nécessaires pour garantir la conformité avec le livre Vème du code. Cela peut inclure la mise en place de nouvelles procédures, la formation du personnel, la modification des systèmes informatiques ou la mise à jour des politiques de confidentialité et des mentions légales

❑Gestion des droits des personnes concernées

La loi accorde plusieurs droits aux personnes concernées, tels que le droit d'accès, de rectification, d'effacement, de limitation du traitement et de portabilité des données. Il est important de mettre en place des mécanismes permettant de traiter les demandes des personnes concernées de manière efficace et conforme aux dispositions du Code.

❑ Nomination d'un délégué à la protection des données (DPO)

Certaines organisations sont tenues de nommer un délégué à la protection des données (DPO) pour superviser et conseiller sur les questions de protection des données. Au cas où une organisation est concernée, elle doit s'assurer de nommer un DPO compétent et de lui fournir les ressources nécessaires pour mener à bien sa mission

❑Réalisation d'analyses d'impact relatives à la protection des données (AIPD)

Dans certains cas, la loi exige la réalisation d'une analyse d'impact relative à la protection des données (AIPD) avant de mettre en œuvre un traitement de données personnelles susceptible d'engendrer un risque élevé pour les droits des personnes concernées. Si l'audit révèle la nécessité de réaliser une AIPD, veillez à suivre les recommandations de APDP

❑ Suivi et mise à jour de l'audit

Un audit réussi ne se limite pas à une opération ponctuelle, mais **nécessite un suivi régulier** pour s'assurer de la conformité continue de l'organisation. Il est donc important de mettre en place des mécanismes de suivi et de révision de l'audit, en tenant compte des évolutions législatives, des changements internes à l'organisation ou des retours d'expérience

JE VOUS REMERCIE