OBLIGATION DE TENUE ET L'ELABORATION DU REGISTRE DES ACTIVITES DE TRAITEMENT

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

SOMMAIRE

REGISTRE DE TRAITEMENT

1. Rôle du DPO

Dans le cadre de la mise en œuvre du principe d'*accountability (conformité à la loi)* , le code du numérique prévoit la désignation, obligatoire, d'un délégué à la protection des données (DPD ou DPO pour *Data Protection Officer*) en application **de l'article 430 du code du numérique.**

Le DPD joue un rôle clé dans la promotion d'une culture de la protection des données au sein de l'organisme et contribue à mettre en œuvre des éléments essentiels tels que les principes relatifs au traitement des données personnelles, les droits des personnes concernées par un traitement, la protection des données dès la conception et la protection des données par défaut, le registre des activités de traitement, la sécurité du traitement ainsi que la notification et la communication des violations de données.

REGISTRE DE TRAITEMENT

1. Rôle du DPO

Plus précisément, il a pour rôle de :

- Veiller au respect des règles grâce à la mise en œuvre d'outils de responsabilité (comme la facilitation d'analyses d'impact relatives à la protection des données et la facilitation ou la réalisation d'audits relatifs à la protection des données) ;

- Servir comme un intermédiaire entre les acteurs concernés (par exemple, l'Autorités de protection, les personnes concernées et les entités économiques au sein d'un organisme).

REGISTRE DE TRAITEMENT

2. <u>Les missions du délégué à la protection des données</u> <u>(Article 432 du code du numérique)</u>

Le DPD a pour mission de :

- **Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent :**

  - Le DPD se voit ainsi confié une mission pédagogique auprès des différents acteurs de l'organisation ;

  - Cette mission peut se traduire par la sensibilisation des parties impliquées dans le traitement et au besoin leur formation.

REGISTRE DE TRAITEMENT

2. <u>Les missions du délégué à la protection des données</u> <u>(Article 432 du code du numérique)</u>

- **Contrôler le respect des dispositions du livre Vème du code du numérique**

- Le contrôle du respect de la loi ne signifie pas que le DPD est personnellement responsable en cas de non-respect de celle-ci ;

- La loi établit clairement que c'est le responsable du traitement, qui est tenu de mettre « en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite » [**Article 387.5 du code du numérique**] et non le DPO.

-

REGISTRE DE TRAITEMENT

2. <u>Les missions du délégué à la protection des données</u> <u>(Article 432 du code du numérique)</u>

- Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;

- Conformément à l'article 428 du code, il incombe au responsable du traitement, et non au DPO, d'effectuer, si nécessaire, une analyse d'impact relative à la protection des données ;

- L'article 428 alinéa 2 recommande que le responsable du traitement demande conseil au DPO sur certaines actions lorsqu'il s'agit d'effectuer une analyse d'impact avant la mise en œuvre d'un traitement. En exemple, le responsable de traitement pourrait être amené à poser des questions telles que :

  - La nécessité ou non de procéder à une analyse d'impact avant la mise en œuvre d'un traitement spécifique ;

REGISTRE DE TRAITEMENT

2. <u>Les missions du délégué à la protection des données</u> <u>(Article 432 du code du numérique)</u>

- .La méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données ;
- La nécessité d'externaliser ou non l'analyse d'impact relative à un traitement des données à la sous-traitant ;
- Les mesures (y compris des mesures techniques et organisationnelles) à appliquer pour atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées par un traitement ;
- Si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et les garanties à mettre en place) sont conformes à la loi

REGISTRE DE TRAITEMENT

2. Les missions du délégué à la protection des données (Article 432 du code du numérique)

- **Coopérer avec l'Autorité de Protection des Données Personnelles (APDP) et faire office de point de contact**

  - Conformément aux dispositions de l'article 432.4 et 5. du code du numérique, le DPD a un rôle de **« facilitateur ».** En effet, il est le point focal de l'Autorité de Protection pour accéder à toute information liée aux traitements des données personnelles au niveau de l'organisation ;

  - Faire des contrôles et réaliser des audits et faire des recommandations sur les mesures correctives.

En cas de désaccord important et persistant sur un point, le responsable de traitement ou le DPD peut s'en référer à l'Autorité de Protection.

REGISTRE DE TRAITEMENT

3. Le registre des activités de traitement

Le registre prévu **par l'article 435 du code** du numérique est outil de gestion des données personnelles qui permet de :

- Piloter et la démontrer la conformité de l'organisation à la loi ;
- Recenser tous les traitements de données et de disposer d'une vue d'ensemble sur tout ce qui est fait en matière de traitement données personnelles ;
- Documenter les traitements de données et de poser les bonnes questions telles que : ai-je vraiment besoin par exemple de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc...

REGISTRE DE TRAITEMENT

3. Le registre des activités de traitement

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard de la loi. Cette étape essentielle permet d'en déduire un plan d'action de mise en conformité des traitements aux règles de protection des données.

Document de recensement et d'analyse, 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 **données personnelles** (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, DRH, santé, etc.) ;

REGISTRE DE TRAITEMENT

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

- les catégories **des personnes concernées** (client, prospect, employé, 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 prévues pour ces transferts ;
- une **description générale des mesures de sécurité** techniques et organisationnelles mis en œuvre ;
- **le délai de conservation** des différentes catégories de données, ou à défaut les critères permettant de le déterminer ;

REGISTRE DE TRAITEMENT

3. Le registre des activités de traitement

Il participe à la documentation de la conformité.

Pour faciliter la tenue du 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 . Il permet de satisfaire au socle d'exigences de la loi .

Il est recommandé, dans la mesure du possible, d'enrichir le registre de mentions complémentaires afin d'en faire un outil plus global de pilotage de la conformité.

Registre des activités de traitement_APDP.x

REGISTRE.ods

REGISTRE DE TRAITEMENT

4. Méthode de renseignement du registre

❑ 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.

❑ Elaborer la liste des traitements

- Faire la liste dans un tableau de suivi, des 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 ;

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

REGISTRE DE TRAITEMENT

4. Méthode de renseignement du registre

❑ 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.

❑ Rappel sur le bonnes pratiques

En enrichissant le registre avec des informations complémentaires, on peut en faire un véritable outil de pilotage de la conformité de l'organisation à la loi. En effet, les obligations de documentation prévues ne se limitent pas seulement à l'obligation de tenir un registre. Disposer, dans un même document, de toutes les informations relatives aux traitements mis en œuvre et exigées par la loi permettra de s'assurer, à chaque instant, de la conformité aux règles de protection des données ou d'identifier les actions qui pourraient être menées pour atteindre cet objectif.

Le registre **pourra également être utilisé par le délégué à la protection des données pour accomplir l'ensemble de ses missions,** voire être consulté par tout collaborateur de l'organisme ayant vocation à mettre en œuvre des traitements de données personnelles

REGISTRE DE TRAITEMENT

4. Méthode de renseignement du registre

Par exemple, **en ajoutant au registre des informations nécessaires pour informer les personnes** (base légale du traitement, et selon le cas, fondement juridique du transfert de données vers des pays tiers, droits qui s'appliquent au traitement, existence ou non d'une décision automatisée, origine des données, etc.), on pourra s'appuyer sur le registre pour rédiger les mentions d'information.

Il sera également possible de **consigner dans le registre un historique des violations de données** et **recenser tous les documents liés aux transferts** de données hors CEDEAO/UEMOA et aux sous-traitants auxquels il est fait recours (contrats de sous-traitance)

REGISTRE DE TRAITEMENT

5. ROLE DU DPO DANS LA CONSTITUTION DU REGISTRE

La loi n'implique pas directement le délégué à la protection des données dans la constitution des registres de traitement . La constitution du registre relève de la responsabilité du responsable de traitement en application des dispositions de l'article 435 alinéa premier. Pour autant, se fondant sur les dispositions de l'article 431 alinéa premier, celles de l'article 432 à savoir , être associé, informer, conseiller et contrôler le respect de la loi, le DPD doit être impliqué étroitement à toutes les questions relevant de la protection des données personnelles.

A ce titre le DPO devrait pouvoir s'impliquer dans la cartographie des traitements de données en vue d'aider à établir le registre en tant que chef d'orchestre de la conformité en matière de données personnelles au sein de l'organisation pour en dégager le plan d'action qui va permettre d'identifier des points de non-conformité à corriger.

REGISTRE DE TRAITEMENT

5. ROLE DU DPO DANS LA CONSTITUTION DU REGISTRE

Toutefois, bien que l'obligation au sens de la loi incombe de manière générale au responsable de traitement ou au sous-traitant, cette tâche peut être confiée à un DPO désigné à cet effet. A ce titre et dès sa prise de fonction, il devra s'atteler à :

- **Identifier au sein de chaque service de l'organisation une personne intéressée par le sujet de la protection des données qui pourrait alors être désignée comme référent sur sa partie métier et ainsi être le point de contact privilégié du DPO pour chaque service**

- **Créer un réseau de personnes plus spécialement désignées pour le seconder dans chaque service dont la mission consistera à :**

  - Remonter des informations auprès du DPO (les traitements de données personnelles réalisés dans leur champ d'action, les catégories de données nécessaires aux traitements, la durée des traitements, méthode de collecte des données de façon opérationnelle, les personnes concernées, mesures de sécurité sont appliquées, etc…);

REGISTRE DE TRAITEMENT

5. ROLE DU DPO DANS LA CONSTITUTION DU REGISTRE

- Relayer les informations et recommandations du DPO auprès des équipes ;

- **Veiller à ce qu'ils soient positionnés de telle sorte qu'ils aient accès aux informations "terrain" ;**

- **S'assurer à ce qu'ils soient en capacité de diffuser** la culture " de protection des données personnelles" au niveau de leur structure ;

- Connaître les procédures pour alerter le DPO ou signaler des incidents.

Ces relais sont les principaux points de contact du DPO au sein de la société et doivent être à même de réagir de manière prompte en cas d'évènement particulier touchant à la protection des données telles que :

REGISTRE DE TRAITEMENT

5. ROLE DU DPO DANS LA CONSTITUTION DU REGISTRE

- Violation de données ;
- Manquement à l'exercice des droit sdes personnes ;
- Analyse d'impact ;
- Contrôle de l'Autorité de Protection.

Certes, il ne s'agit pas d'en faire des DPO bis, mais plutôt de leur donner les moyens de se poser les bonnes questions et de relayer les bonnes informations aux bonnes personnes.

REGISTRE DE TRAITEMENT

6. Constitution du registre par le DPO : comment procéder ?

- Identifier les points positifs et lacunes au regard des principes la loi sur la protection des données personnelles et les diverses lignes directrices et recommandations adressées par l'APDP s'il a lieu ;

- Réaliser une évaluation de maturité visant à obtenir une première estimation de l'ampleur des tâches à venir en se poser des questions simples traduisant les exigences de la législation. Parmi ces questions réparties en plusieurs catégories, on pourrait par exemple retrouver de manière non-exhaustive les points de contrôle suivants :

  - **sur la gouvernance :**

  - Existe-t-il des politiques de protection des données personnelles des clients, usagers, prospects, salariés, etc… ;

  - Le personnel a-t-il été sensibilisé aux enjeux de la protection des données personnelles et à la sécurité informatique ?

  - Existe-t-il une procédure en cas de contrôle de l'Autorité ?

REGISTRE DE TRAITEMENT

6. Constitution du registre par le DPO : comment procéder ?

❑ **Sur le Registre des traitements :**

- Les traitements de données personnelles ont-ils été recensés ?

- Un registre des traitements a-t-il été constitué ?

❑ **Sur les données personnelles :**

Les traitements identifiés ont une finalité déterminée, explicite et légitime ;

- Les traitements impliquant l'utilisation de données sensibles ont été identifiés.

❑ **Sur la gestion des risques :**

- Les traitements nécessitant une analyse d'impact relative à la vie privée ont-ils été identifiés ?

REGISTRE DE TRAITEMENT

6. Constitution du registre par le DPO : comment procéder ?

❑ Sur la Transparence :

Les personnes concernées par les traitements sont-elles correctement informés de ceux-ci ?

❑ Sur la Sous-traitance :

- Les relations avec les sous-traitants sont-elles encadrées par un contrat écrit ?

❑ Sur la sécurité :

- Une charte informatique a-t-elle été adoptée et communiquée à l'ensemble du personnel ?

REGISTRE DE TRAITEMENT

6. Constitution du registre par le DPO : comment procéder ?

Pour obtenir les réponses aux questions qu'il a prédéfinies, le DPO devra être à même de solliciter les membres de son réseau interne orienté métiers de l'entreprise, pouvoir accéder à de la documentation de l'organisme, tout ceci afin de mesurer et obtenir un premier indicateur du niveau de maturité de celui-ci.

- **Comment constituer un registre ?**

La mission préalable à l'élaboration du registre est le recensement des informations nécessaires à sa constitution ce qui nécessite de rencontrer les responsables opérationnels des divers services. Le site web doit également être analysé pour identifier les traitements effectués sur cet environnement.

REGISTRE DE TRAITEMENT

6. Constitution du registre par le DPO : comment procéder ?

Si les collaborateurs sont sensibilisés à la protection des données personnelles ils seront à même d'identifier les traitements de manière autonome et donner leurs caractéristiques principales. La transmission d'une documentation à compléter pourra être envisagée dans ce cas afin d'être plus rapide lors des entretiens. Le cas échéant, il faudra prévoir à l'occasion des entretiens un temps de présentation des enjeux du registre et définir les notions clés de la loi avant d'interroger les collaborateurs sur leurs activités de traitement.

Les entretiens doivent donner lieu à une fiche de traitement par activité, un traitement correspondant à une finalité précise et non à l'utilisation d'un logiciel spécifique car ce logiciel peut être utilisé pour divers traitements.

Une fois que ces informations sur les traitements sont collectées, une liste des traitements par activité doit être dressée selon que le traitement concerne le service des ressources humaines, la logistique, l'accueil etc….

REGISTRE DE TRAITEMENT

6. Constitution du registre par le DPO : comment procéder ?

Une fois la majorité des traitements recensés, les volets du registre de traitement peuvent être affinés et précisés afin de fournir un degré de détail plus important.

Le registre peut ensuite être analysé pour déterminer quels sont les risques qui pèsent sur les traitements de données et procéder à l'élaboration d'un plan d'action de mise en conformité des traitements.

❑ La tenue régulière du registre ?

Il n'y a pas de version définitive du registre des activités de traitements. Celui-ci doit être mis à jour régulièrement en tenant compte des nouvelles activités de l'entreprise, du déploiement d'une branche de l'activité, de l'acquisition d'un nouveau logiciel etc. Les évolutions organisationnelles et techniques doivent être prises en compte et ainsi les caractéristiques du traitement doivent être adaptées concernant : les données traitées, les durées de conservation, les destinataires, etc.

REGISTRE DE TRAITEMENT

7. Définition d'un plan d'actions et priorisation.

Apporter des réponses à ces interrogations et identifier le niveau de maturité de l'organisme permettront bien évidemment de dégager un plan structuré visant à définir et prioriser des actions de remédiation aux lacunes constatées.

Bien entendu, ce premier plan d'actions dégagé suite à cette évaluation de la maturité continuera d'être alimenté au fur et à mesure de l'avancement du projet de conformité.

REGISTRE DE TRAITEMENT

7. Définition d'un plan d'actions et priorisation.

Par exemple, le registre permettra de mettre le doigt sur l'absence de durées de conservation des données, allant ainsi à l'encontre du principe de limitation des données. Autre exemple, la constitution des fiches de traitements avec les métiers pourra également être utile pour constater le défaut d'information des personnes concernées.

Tous ces éléments viendront alimenter les actions qui devront être déployées au fur et à mesure de l'avancement de la conformité.

REGISTRE DE TRAITEMENT

8. Le suivi dans le temps

Tout le long de la vie du projet de conformité de l'entreprise, qui vivra aussi longtemps que l'organisation elle-même, le DPO et son équipe devront s'assurer de mettre en place un suivi à long terme.

Cela passera par la qualification d'actions dites "*quickwin*", dont la mise en place permettra d'avoir un fort impact sur le taux d'avancement de la conformité tout en limitant le temps nécessaire à leur implémentation.

Toutes ces actions qui constituent le plan de conformité de l'entreprise devront donc être priorisées en fonction de leur difficulté, de la charge qu'elles représentent et de l'impact qu'elles auront sur le niveau de maturité de l'entreprise.


JE VOUS REMERCIE POUR VOTRE
ATTENTION