AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES (APDP)

FORMATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES PERSONNELLES

Thème 1 : Les relations du DPDP avec l'autorité de contrôle

Intervenant : Professeur ZANNOU Martial Tiburce

19 Décembre 2022

INTRODUCTION

Le délégué à la protection des données, aussi appelé DPO pour « Data Protection Officer », est la personne en charge de la protection des données à caractère personnel au sein des organismes publics ou privés.

Pour les organismes dont la désignation est obligatoire, il sera le conseiller et l'intermédiaire privilégié pour piloter la conformité. Au sein de l'organisme, le DPO sera également l'interlocuteur privilégié pour toutes les questions relatives aux données personnelles, qu'elles soient internes ou qu'elles émanent d'une personne concernée par un traitement effectué par l'organisme.

Le métier de délégué à la protection des données (« DPD », ou « DPO ») est devenu essentiel. Depuis l'avènement de la loi 2017-20 portant code du numérique en République du Bénin. Désormais, le traitement de données personnelles est une composante fondamentale de la plupart des secteurs d'activité. Dès lors, le DPO prend une importance qualitative et quantitative. L'évolution est qualitative, tout d'abord : l'esprit du règlement est de faire du DPO le personnage central de la gestion des données personnelles dans l'organisme qui le désigne. Le positionnement hiérarchique du DPO doit en témoigner, et ses ressources doivent être adaptées, afin qu'il puisse accomplir pleinement son métier et son rôle de pilote de la conformité. Il ne doit pas travailler en vase clos, mais être pleinement intégré aux activités opérationnelles de son organisme. Il est un maillon essentiel de la gouvernance de la donnée.

Quelles relations un DPD entretient avec l'autorité ?

En tant que point focal de la gouvernance des données, le DPD doit travailler en parfaite symbiose avec l'autorité des données à caractère personnel. Cela induit un certain nombre d'obligations.

<u>Section1</u> - Obligations générales et modalités du contrôle

Le DPO veille à la **conformité** de son organisme au regard de la réglementation applicable en matière de protection des données personnelles. À ce titre, il doit :

- **Informer et conseiller**
- **Contrôler le respect** de la règlementation
- **Dispenser des conseils**
- **Coopérer avec l'autorité**
- **Faire office de point focal pour l'autorité.**

Le DPO est donc une fonction **essentielle et fortement recommandée** pour permettre à un organisme traitant des données personnelles de s'assurer qu'il respecte la réglementation applicable dans le cadre de la protection des données personnelles et de la vie privée.

Le DPO accompagne son organisme dans sa mise en conformité, et dans le maintien de celle-ci dans le temps. **De façon synthétique** cela implique conformément aux dispositions de **l'article 432** de la loi portant code du numérique en République du Bénin :

- **d'aider** l'organisme à cartographier ses traitements ;
- **de prioriser** les actions à mener en matière de protection des données en fonction du contexte et des risques associés ;
- **d'organiser** les procédures internes visant à gérer les traitements de données personnelles, les éventuelles demandes d'exercice de droits et violations ;
- **de documenter** la conformité de l'organisme, afin qu'en cas de contrôle, celui-ci puisse aisément démontrer sa conformité à la réglementation applicable.

A- Les missions du délégué à la protection des données (Article 432)

Article 432 Les missions du délégué à la protection des données sont au moins les suivantes :

1. 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 en vertu des dispositions du présent Livre en matière de protection des données ;

2. contrôler le respect des dispositions du présent Livre en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

3. 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 en vertu de **l'article 428 (la teneur de cet article est mise en évidence dans les développements à suivre)** ;

4. coopérer avec l'Autorité ;

5. faire office de point focal pour l'Autorité sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 412, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

- Clarifications conceptuelles :

En droit il existe trois types d’obligations : l’obligation de moyen et de résultat, et obligation de sécurité.

- **De lege lata, l'obligation de moyens** consiste en l'engagement obligatoire du débiteur à mettre en œuvre tous les moyens nécessaires et dont il dispose pour réaliser les objectifs et prestations de services prévus au contrat.

- **L'obligation de résultat** désigne l'obligation en vertu de laquelle le débiteur s'engage à procurer un résultat déterminé au créancier. Il ne s'engage pas simplement à faire ses meilleurs efforts pour essayer d'atteindre le résultat, il s'engage à l'atteindre.

- **L'obligation de sécurité** est une obligation de résultat et le simple fait de ne pas arriver à ce résultat suffit à engager sa responsabilité. Ce manquement peut faire l'objet d'une condamnation pénale au tribunal correctionnel.

- Comment savoir si c’est une obligation de moyen ou de résultat ?

L'obligation de moyens signifie que le débiteur doit mettre en œuvre toutes les ressources qu'il a à sa disposition pour accomplir la prestation convenue, sans pour autant garantir le résultat. Tandis qu'avec l'obligation de résultat, ce qui compte c'est que le résultat soit atteint.

L'obligation désigne le lien de droit entre deux ou plusieurs personnes.

En effet, dans le cas d'une obligation de moyen, la responsabilité du prestataire n'est pas engagée si le résultat n'est pas atteint. De lege lata, l'obligation de moyens consiste en l'engagement obligatoire du débiteur à mettre en œuvre tous les moyens nécessaires et dont il dispose pour réaliser les objectifs et prestations de services prévus au contrat. Dans le cas d'une obligation de résultat, sa responsabilité est engagée dès que le résultat n'est pas atteint.

Ces clarifications notionnelles permettent d'appréhender de manière plus explicite les différentes obligations mises à la charge du DPD.

L'obligation de veiller à la conservation des données à caractère personnel, conformément aux dispositions pertinentes de l'article 433 du code du numérique en République du Bénin.

Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

B- Les obligations de conservation (article 433)

Article 433 : Les obligations de conservation

Les données à caractère personnel ne doivent pas être conservées au-delà de la période requise pour les fins en vue desquelles elles ont été recueillies et traitées.

Au-delà de cette période requise, les données ne peuvent faire l’objet d’une conservation qu’en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales. Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d’archives sont dispensés des formalités préalables à la mise en œuvre des traitements prévus par les dispositions du présent Livre.

Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées à l’alinéa 2 :

- soit avec l’accord exprès de la personne concernée ;

- soit avec l’autorisation de l'Autorité.

Obligation de pérennité : Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées, quel que soit le support technique utilisé.

C- Les obligations de pérennité (Article 434)

Article 434 : Les obligations de pérennité

Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées, quel que soit le support technique utilisé.

Il doit particulièrement s’assurer que l’évolution de la technologie ne sera pas un obstacle à cette exploitation.

Section 2 – Le dossier d'accountability

L’accountability est un principe désignant l’obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».

Le principe d’accountability peut se traduire en français par la notion de « responsabilisation ».

L’accountability est un principe issu de l’article 428 du Code du numérique en République du Bénin, désignant « l’obligation pour les personnes physiques, le responsable du traitement de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».

En synthèse, l’accountability implique, pour les organismes traitant des données personnelles :

- De déployer les mesures appropriées (techniques, organisationnelles, contractuelles, etc.) pour se conformer au Régime de Protection de Données à Caractère Personnel ;

- D’être en mesure de démontrer sa conformité au Régime de Protection de Données à Caractère Personnel.

Cette démonstration se base notamment sur la production d’une documentation exhaustive et détaillée, décrivant l’ensemble des procédures et des bonnes pratiques appliquées par l’organisme en matière de données personnelles.

A- Les outils de conformité

1- Analyse d’impact : (Article 428 alinéa 1 à 2)

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

L'analyse d'impact relative à la protection des données visée à l’alinéa 1er est, en particulier, requise dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

- le traitement à grande échelle de catégories particulières de données visées à l'article 394, alinéa premier, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395 ; ou

- la surveillance systématique à grande échelle d'une zone accessible au public.

L'Autorité établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément à l’alinéa 1er.

L'Autorité peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise conformément à l’alinéa 1er..

L'Autorité peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

L'analyse contient au moins :

1. une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;

2. une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;

3. une évaluation des risques pour les droits et libertés des personnes concernées conformément à l'alinéa 1 ; et

4. les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect des dispositions du présent Livre, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

2- Registre des traitements

- **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.

- **<u>Contenus d'un registre</u>**

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 effectués.

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.) ;
- 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 ;

Article 435 : Registre des activités de traitement

Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

1. le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

2. les finalités du traitement ;

3. une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

4. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

5. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale ;

6. les délais prévus pour l'effacement des différentes catégories de données ;

7. une description générale des mesures de sécurité techniques et organisationnelles.

Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

1. le nom et les coordonnées du ou des sous- traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

2. les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

3. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts, les documents attestant de l'existence de garanties appropriées ;

4. une description générale des mesures de sécurité techniques et organisationnelles.

Les registres visés aux alinéas 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'Autorité sur demande.

Les obligations visées aux alinéas 1 et 2 ne s'appliquent pas aux petites et moyennes entreprises sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 394, alinéa premier, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions.

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.

- **<u>Méthode de renseignement du registre</u>**

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.

Élaborer 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 ;

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

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'action de mise en conformité à la loi.

3- Encadrement des transferts (article 391)

Le transfert de données à caractère personnel faisant l'objet d'un transfert vers un État tiers ou une organisation internationale ne peut avoir lieu que lorsque l'Autorité constate que l'État ou l'Organisation internationale en question assure un niveau de protection équivalent à celui mis en place par les dispositions du présent Livre.

Article 391 : Transfert de données à caractère personnel vers un État tiers ou une organisation internationale

- Règles générales

Le transfert de données à caractère personnel faisant l'objet d'un transfert vers un État tiers ou une organisation internationale ne peut avoir lieu que lorsque l'Autorité constate que l'État ou l'Organisation International en question assure un niveau de protection équivalent à celui mis en place par les dispositions du présent Livre.

Le caractère équivalent et suffisant du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données.

Afin de déterminer ce caractère équivalent et suffisant, il est notamment tenu compte de :

1. l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, notamment dans le domaine de la sécurité publique, de la défense, de la sécurité nationale et du droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;

2. l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres de la Communauté économique des États de l’Afrique de l’Ouest ; et

3. les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

Avant tout transfert effectif de données à caractère personnel vers un État tiers ou une organisation internationale, le responsable du traitement doit préalablement obtenir l’autorisation de l'Autorité.

Les transferts de données à caractère personnel vers des États tiers ou une organisation internationale font l’objet d’un contrôle régulier de l'Autorité au regard de leur finalité.

4- Certifications ou codes de bonne conduite

Les certifications ou codes de conduites sont l’un des nouveaux outils de conformité.

<u>Section 3</u> – L’élaboration du rapport d’activité annuel

Le rapport d’activité annuel est une obligation légale qui a pour finalité de se conformer aux contenus des exigences de **l’article 387 de la loi 2017-20 portant code du numérique en République du Bénin.**

L’article 387 point 14 dernier alinéa de la loi 2017-20 portant code du numérique en République du Bénin.

Le responsable du traitement est tenu d’établir un rapport annuel pour le compte de l'Autorité concernant le respect des alinéas 1 et 2.

1. faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 383, 389, 395, 396 et 397 du présent code

2. veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service ;

Article 383 : Conditions générales de licéité des traitements de données à caractère personnel

Article 389 : Principe du consentement et de légitimité

Article 395 : Données à caractère personnel relatives aux condamnations pénales et aux mesures de sûreté connexes

Article 396 : Données à caractère personnel à des fins historiques, statistiques ou scientifiques

Article 397 : Données à caractère personnel aux fins de journalisme, de recherche, d’expression artistique ou littéraire.

Section 4 – Régime de responsabilité du DPDP

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

À défaut sa responsabilité ou celle de son représentant personnel peut-être engagé.

On distingue plusieurs types de responsabilités :

1- Responsabilité civile

La responsabilité civile vise à réparer un dommage subi par autrui. La responsabilité civile crée l'obligation de réparer le dommage causé.

Tout dommage causé à autrui doit être réparé. Ainsi, la responsabilité civile est engagée dans de très nombreux cas : lors de dommages provoqués par soi-même, par ses enfants mineurs ou par ses préposés dans l'exercice de leurs activités (femme de ménage, baby-sitter, jardinier…). Elle peut aussi être engagée par « les choses dont on a la garde » (chute d'une tuile du toit par exemple).

3 conditions sont nécessaires pour qu'il y ait responsabilité civile :

- un dommage subi par la victime,
- un fait dit « générateur de responsabilités » imputé à l'auteur de ce dommage,
- un lien de causalité entre ce fait et le dommage.

2- La responsabilité pénale

La responsabilité pénale, dans les cas où il y a infraction aux dispositions pénales même en dehors de tout préjudice subi par un tiers. La responsabilité pénale a pour finalité de réprimer l'auteur des faits. Une sanction pénale est donc prononcée ; la responsabilité civile a, quant à elle, pour objet de réparer le dommage qu'il a causé. Dans ce cas, la condamnation porte sur l'allocation de dommages et intérêts à la victime.

3- La responsabilité internationale

Il ressort des principes généraux de la protection des données à caractère personnel que le développement de l’informatique doit s'opérer dans le cadre de la coopération internationale et il ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

4- La responsabilité administrative

La responsabilité administrative désigne l'obligation qui incombe à l'administration de réparer les dommages occasionnés par son action ou son inaction. L’individualisation de la responsabilité par acteur. Il sera question d’identifier les acteurs sur la tête de qui repose une quelconque responsabilité, selon le livre cinquième.

CONCLUSION

Les missions du DPD demandent des compétences juridiques et informatiques. Pour mener à bien ces tâches, le DPD doit avoir des qualités humaines et organisationnelles. Ses atouts lui permettront de réussir ses missions.

C’est pour vous accompagner dans votre mise en conformité, que l’APDP vous propose des formations adaptées à tous.

Le délégué à la protection des données doit agir de manière indépendante dans l’entreprise et ne doit pas recevoir d’instructions concernant l’exercice de ses missions. Il ne peut être pénalisé ou relevé de ses fonctions par le responsable de traitements pour l’exercice de ses missions car le respect des obligations en matière de protection des données relève de la responsabilité du responsable du traitement.

Le responsable de traitement doit mettre certains moyens à disposition du DPD afin que celui-ci puisse garantir la bonne réalisation de ses missions et remplir son rôle de DPD. Entre autres moyens la direction doit mettre à disposition du DPD :

- Un outil de management des activités afin de lui faciliter la saisie du registre de traitement et la rédaction des bilans
- Permettre au DPD de solliciter à tout moment les services de l’entreprise qu’il juge utile en vue d’un soutien et d’un accompagnement

Le délégué à la protection des données peut être un membre du personnel du responsable de traitement, donc il s’agit d’un DPD interne à l’entreprise. Il peut également exercer ses fonctions sur la base d’un contrat de service, on parle donc d’un DPD externe. La loi n’impose aucune contrainte à ce sujet, l’entreprise peut désigner ou recruter un DPD en interne ou externaliser cette fonction à un expert.

Le DPD interne :

Un délégué à la protection des données interne à l’entreprise connaît le domaine d’activité et l’environnement de travail de la structure où il opère. Il connaît également les interlocuteurs et valeurs de l’entreprise. En interne, le DPO sera plus réactif en cas de besoin immédiat.

Le DPD externe :

Le DPD externe est neutre et indépendant ce qui permet d’éviter le risque de conflit d’intérêt. Il peut être disponible immédiatement car il n’a pas besoin d’être formé à ce poste.

MERCI POUR VOTRE AIMABLE ATTENTION