AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES (APDP)

FORMATION DES DELEGUES A LA PROTECTION DES DONNEES PERSONNELLES

Thème 1 : *DPO - Rôle et mise en place*

Intervenant : Professeur ZANNOU Martial Tiburce

décembre 2023

Sommaire

- ***Section 1*** : Protection des données personnelles: champs d'application et notions
- ***Section 2*** : Les grands principes de la protection des données personnelles
- ***Section 3*** : Profil de poste
- ***Section 4*** : Modalités de désignation et mise en place.

INTRODUCTION : Protection des données personnelles au Bénin

La question du traitement des données à caractère personnel apparaît comme un enjeu économique majeur. La quantité de données collectées augmente chaque année et sera au cœur de l'économie de demain.

L'évolution des nouvelles technologies permettant de recueillir, de traiter, de stocker, de rechercher et de diffuser des informations, les traces que leur simple usage génère, la valeur marchande acquise par les informations ; les fichiers se vendent d'autant plus cher qu'ils sont enrichis et permettent d'établir des profils ; le développement d'Internet, l'internationalisation des échanges concourent à une "libre circulation" des données personnelles, et doivent conduire les citoyens que nous sommes à une vigilance accrue du respect de la vie privée et des libertés individuelles. En cela, la protection des données personnelles est devenue un enjeu quotidien.

Section 1 : Protection des données personnelles: champs d'application et notions

I- Champ d'application du code du numérique

Le code du numérique a un champ d'application large. Au terme de l'article 2, il a pour objet de régir :

- les activités qui relèvent des réseaux et services de communications électroniques ;
- les outils électroniques ;
- les services de confiance en l'économie numérique ;
- le commerce électronique ;
- *la protection des données à caractère personnel* ; et
- la cybercriminalité et la cybersécurité

II- Champ d’application du livre Vième

Le champ d’application d’une loi est la détermination des limites dans lesquelles cette loi s'applique. On distingue le champ d’application matériel et le champ d’application territorial.

A-/ Champ d’application matériel

L’expression "Ratione materiae" signifie "en raison des dispositions légales ou règlementaires qui règlent la matière.

La notion de compétence matérielle recouvre toutes les classes d’affaires dont un tribunal peut connaître. En d’autres termes, il s’agit de la compétence « s’appréciant en raison de l’objet du litige ». Chaque tribunal peut entendre une classe particulière d’affaires : des affaires liées à des litiges de droit du travail ; des affaires liées à l’interprétation ou à la violation de la constitution ; des affaires touchant au droit civil.

Il en va de même du livre Vième qui régit la matière de protection des données personnelles.

Aux termes de l'article 380, les dispositions du livre Vième s'appliquent notamment à :

1- toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation de données à caractère personnel par une personne physique, par l'État, les collectivités locales, les personnes morales de droit public ou de droit privé ;

2- tout traitement automatisé en tout ou en partie, ainsi que tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l'exception des traitements visés à l'alinéa 2 ;

3- tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté et les intérêts essentiels de l'État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Toute collecte, traitement, transmission, stockage, et usage de données à caractère personnel restent toutefois soumis aux dispositions nationales, communautaires, régionales et internationales applicables en matières commerciale, civile et pénale.

B-/ Champ d’application territorial de la loi

L'expression latine "ratione loci" signifie " en raison du lieu". Elle est employée dans les affaires dans lesquelles est soulevée un moyen portant sur la compétence géographique d'une juridiction

Aux termes de l’article 381, les dispositions du Livre Vième s'appliquent au traitement des données à caractère personnel effectué dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant sur le territoire de la République du Bénin, que le traitement ait lieu ou non en République du Bénin.

Les dispositions du livre s'appliquent au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de la République du Bénin par un responsable du traitement ou un sous-traitant qui n'est pas établi en République du Bénin, lorsque les activités de traitement sont liées :

1- à l'offre de biens ou de services à ces personnes concernées en République du Bénin, qu'un paiement soit exigé ou non desdites personnes ; ou

2- au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de la République du Bénin ;

3- le traitement est mis en œuvre sur le territoire d’un Etat membre de la CEDEAO.

Les dispositions du présent Livre s'appliquent au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi en République du Bénin mais dans un lieu où le droit de la République du Bénin s'applique en vertu du droit international public

III- Quelques définitions

Clarifions quelques concepts importants en matière de protection des données :

- **Collecte en temps réel :** rassemblement des preuves contenues dans des communications en cours de production, lequel rassemblement est réalisé au moment de la transmission de la communication ;

- **Données à caractère personnel :** toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée. Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

- Données afférentes à la création de signature : données uniques telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique sécurisée ;

- Données biométriques : toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques,

- Données concernant la santé : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

- Données de création de cachet électronique : données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

- Données d'identification personnelle : ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

- **Données génétiques :** toute information concernant les caractères génétiques héréditaires ou acquis d'une personne physique qui donnent des indications uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;

- **Données informatiques :** toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

- **Données relatives aux abonnés :** toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

▪ le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

- l’identité, l’adresse postale ou géographique et le numéro de téléphone de l’abonné, et tout autre numéro d’accès, les données concernant la facturation et le paiement, disponibles sur la base d’un contrat ou d’un arrangement de services ;

- toute autre information relative à l’endroit où se trouvent les équipements de communication, disponible sur la base d’un contrat ou d’un arrangement de services.

- Données relatives au contenu : contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication. Il s'agit de tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic ;

- Données relatives au trafic : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu’élément de la chaîne de communication, indiquant l’origine, la destination, l’itinéraire, l’heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

- **Données sensibles :** toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, à la génétique, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

- **Fichier :** tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

- **Profilage :** toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

- Responsable du traitement : toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens;

- Sous traitant : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement;

- Stockage de données : utilisation de supports d'enregistrement pour la conservation de données à l'aide d'ordinateurs ou d'autres devices. Les formes les plus courantes de stockage de données sont le stockage de fichier, le stockage de bloc et le stockage d'objet, chaque procédé étant la solution optimale pour un objectif particulier;

- Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, le cryptage, l'effacement ou la destruction.

- **Traitement automatique ou automatisé de données informatiques :** ensemble des opérations réalisées en totalité ou en partie par des moyens automatisés, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'application d'opérations logiques et/ou arithmétiques l'édition des données et d'une façon générale, leur exploitation sans intervention humaine directe

- **Transmission :** tous les transferts de données, par téléphone, télécopie, courriel ou transfert de fichiers.

Section 2 : Les grands principes de la protection des données personnelles

Les données à caractère personnel doivent être :

1- traitées légitimement ;

2- collectées, enregistrées, traitées, stockées et transmises de manière licite, loyale, transparente et non frauduleuse ;

3- collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ;

4- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

5- exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

6- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées.

Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 396, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par les dispositions du présent Livre afin de garantir les droits et libertés de la personne concernée ;

7- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Il incombe au responsable du traitement d'assurer le respect de l'alinéa premier.

Le cas particulier du consentement

Le consentement est un concept central : tout résident de le territoire doit avoir donné explicitement son consentement pour que ses données à caractère personnel puissent être collectées, traitées et conservées.

Pour appuyer cette exigence, le règlement restreint la portée du système de consentement explicite. Il stipule que ces données doivent être collectées pour une finalité prédéfinie et très spécifique. Toute personne concernée doit être clairement informée de cette finalité. Redonner au citoyen le contrôle de ses données. L'exigence de loyauté de ce principe reconnaît à tous les résidents, le « droit à l'oubli », ce qui signifie qu'ils peuvent obtenir sur demande la suppression de leurs données à caractère personnel de toutes les banques de données du responsable du traitement (et de celles de ses sous-traitants). Quant à l'obligation de transparence, elle confère à chaque résident le « droit d'accéder » à toutes les données personnelles le concernant détenues par le responsable du traitement. La personne concernée peut demander une copie de toutes ses données dans un format numérique, structuré et couramment utilisé, et sa demande devra être satisfaite dans le mois qui suit sa réception.

L’encadrement de la prospection commerciale

- La prospection commerciale est un outil indispensable pour l’entreprise. Omniprésente auprès des consommateurs, elle n’en reste pas moins importante auprès des professionnels. Dans un contexte d’économie numérique, comment prospecter en toute conformité ?

- Les règles en matière de prospection commerciale consacrent le principe du recueil du consentement préalablement à toute prospection commerciale par voie électronique (e-mail, SMS et fax)

- La personne concernée doit alors donner son consentement pour la prospection commerciale au moment de la collecte de ses données personnelles. Le recueil du consentement est souvent matérialisé par une mention du type « En cochant cette case, vous acceptez de recevoir des propositions commerciales par voie électronique ».

- Le recours aux cases pré-cochées est à proscrire, puisque le consentement doit être univoque, c’est-à-dire qu’il doit résulter d’un acte positif. De plus, le consentement ne vaut que pour la personne pour laquelle il est recueilli.

- Le code du numérique prône la transparence : si les données de la personne concernée sont susceptibles d’être transmises ou cédées à des partenaires, elle devra en être informée au préalable.

- Pour être valable, le consentement doit être spécifique, c’est-à-dire donné pour une finalité spécifique (un objectif donné), il faudra donc prévoir une autre case à cocher pour la transmission à des tiers (le consentement doit être donné pour chacune des finalités de la collecte). Il n’est pas possible d’utiliser les données recueillies aux fins de prospection pour une autre finalité.

- **Dérogation à la prospection commerciale : le droit d’opposition**

Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, autrement que par écrit, le responsable du traitement demande à celle-ci si elle souhaite exercer le droit d'opposition, soit sur un document qu'il lui communique à cette fin au plus tard soixante (60) jours après la collecte des données à caractère personnel, soit par tout moyen technique qui permet de conserver la preuve que la personne concernée a eu la possibilité d'exercer son droit.

En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d’accès sauf lorsqu’il est établi que les données contestées ont été communiquées par l’intéressé ou avec son accord.

Lorsque des données à caractère personnel sont collectées par écrit, que ce soit sur un support papier, support électronique ou tout autre support équivalent, auprès de la personne concernée, le responsable du traitement demande, à celle-ci, sur le document grâce auquel il collecte ses données, si elle souhaite exercer le droit d'opposition.

Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, autrement que par écrit, le responsable du traitement demande à celle-ci si elle souhaite exercer le droit d'opposition, soit sur un document qu'il lui communique à cette fin au plus tard soixante (60) jours après la collecte des données à caractère personnel, soit par tout moyen technique qui permet de conserver la preuve que la personne concernée a eu la possibilité d'exercer son droit.

En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d’accès sauf lorsqu’il est établi que les données contestées ont été communiquées par l’intéressé ou avec son accord.

- **Le principe de transparence**

- Article 384 : Principe de transparence : information et consentement de la personne concernée

- Les modalités d'information devant être respectées afin d'obtenir le consentement éclairé des personnes impactées par la collecte de données, ainsi que d'appréhender les droits découlant de la collecte de ces données doivent être bien connues. Il s'agit de :

a) L'information de la personne concernée

1) Informations à fournir au moment de la collecte

- identité et coordonnées du responsable du traitement ;

- coordonnées du DPO ;

- finalités du traitement ainsi que la base juridique du traitement ;

- information sur les intérêts légitimes de la collecte ;

- les destinataires ou les catégories de destinataires de la collecte ;

- la durée de conservation (ou si imprévisible : critère de fixation de la durée) ;

- informations sur le droit de la personne sur ses données collectées (accès, suppression, rectification, limitation….) ;

- le droit d'introduire une réclamation auprès de l'autorité ; sur le caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et sur les conséquences sur la non-fourniture des données ;

- sur l'existence d'une prise de décision automatisée ;

- si traitement ultérieur : information sur la nouvelle finalité.

Il n'est pas nécessaire de fournir les informations si la personne concernée dispose déjà de celles-ci.

2) Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée:

- si le responsable du traitement a l'intention d'effectuer un transfert des données à un destinataire dans un pays tiers ou à une organisation internationale et les garanties appropriées ;

- La source d’où proviennent les données (si source accessible ou non au public).

Le délai pour fournir ces informations :

- délai raisonnable après l’obtention des données à caractère personnel : maximum 1 mois ;

- si les données doivent être utilisées aux fins de communication avec la personne concernée : au plus tard au moment de la communication ;

- si les données sont destinées à un autre destinataire : au plus tard au moment la première communication.

Aucune information n’est nécessaire si :

la personne concernée dispose déjà de ces informations ;

la fourniture de telles informations se révèle impossible ou exigerait un effort disproportionné ;

la collecte est prévue par la loi ;

les données sont confidentielles (ex : obligation légale découlant du secret professionnel).

b) L’obtention du consentement

Le consentement est défini comme « toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Pour traiter les données personnelles d’une personne, son consentement préalable doit toujours être obtenu, sauf en cas de :

- contrats et mesures précontractuelles : quand il s’agit d’une relation avec un client ou prospect (par exemple en créant un compte sur internet) ;

- obligation légale du responsable de traitement (ex : l’employeur) ;
- sauvegarde de la vie humaine ;
- mission de service public (ex : les impôts) ;
- intérêt légitime du responsable de traitement.

Le consentement doit être :

- libre ;

- démontré : il faut garder une preuve du consentement. Il faut une traçabilité (ex : signature, empreinte vocale, code envoyé par téléphone…) retiré aussi facilement qu'il a été donné. Cela peut se faire par écrit (y compris voie électronique) ou par oral

- éclairé et univoque

c) Les droits de la personne concernée

1) Droit d'accès

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées, ainsi qu'un droit d'accès aux données.

Copie des données.

2) Droit de rectification

La personne concernée a le droit à la rectification des données qui sont inexactes ou incomplètes dans les meilleurs délais.

3) Droit à l'effacement et à l'oubli

Le droit à l'effacement dans les meilleurs délais s'applique si :

- les données personnelles ne sont plus nécessaires au regard de la finalité du traitement ;

- retraitement du consentement ;

- opposition au traitement ;

- le traitement est illicite ;

- effacement afin de respecter une obligation légale ;

- les données personnelles sont collectées sur le fondement de l'article 8, 1 (sur le consentement des enfants) ;

- Les données à caractère personnel ont été rendues publique et que le responsable du traitement est tenu de les effacer. Il doit prendre des mesures raisonnables y compris d'ordre technique, pour informer les tiers responsables du traitement sur cette demande d'effacement.

Il n'y a pas de droit à l'effacement dans les hypothèses suivantes :

- exercice du droit à la liberté d'expression et d'information ;

- pour respecter une obligation légale ;

- motifs d'intérêts publics ;

- à des fins archivistiques ;

- nécessaire à la constatation, à l'exercice ou à la défense en justice.

4) Droit à la limitation du traitement

La personne concernée par le traitement peut obtenir la limitation du traitement si l'un des éléments suivants s'applique si :

- l’exactitude des données est contestée par la personne (le responsable du traitement dispose d’un délai de vérification) ;

- le traitement est illicite (limitation sauf si la personne souhaite l’effacement) ;

- les données ne sont plus nécessaires pour le responsable du traitement mais nécessaire pour la personne concernée pour la constatation, l’exercice ou la défense en justice (action en justice) ;

- l’opposition de la personne, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

5) Droit de notification

Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation.

6) Portabilité

- Droit d’obtenir les données dans un format structuré, couramment utilisé et lisible par une machine ;

- Droit de transférer les données directement auprès d’un nouveau responsable du traitement.

7) Droit d’opposition

- La personne concernée peut s’opposer à tout moment, pour des raisons personnelles, au traitement de ses données y compris pour le profilage ;

- L’exercice du droit d’opposition implique que le responsable du traitement évalue le droit de la personne concernée au non traitement de ses données et les motifs légitimes du responsable du traitement de poursuivre ce traitement malgré cette opposition ;

- Le responsable du traitement doit informer la personne concernée de son droit d'opposition « au plus tard au moment de la première communication avec la personne concernée » ;

- Les personnes concernées peuvent s'opposer, mais il ne sera pas fait droit à leur demande d'opposition si le traitement est « nécessaire à l'exécution d'une mission d'intérêt public ».

8) Profilage

- Droit de ne pas faire l’objet d’une décision fondée exclusivement sur un traitement automatisé, y compris du profilage, sauf si cela est :

autorisé par la loi ;

- « nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement » ;

fondé sur le consentement explicite de la personne.

- Le responsable du traitement doit mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne.

Le principe de transparence implique une information obligatoire et claire ainsi qu’intelligible de la part du responsable du traitement portant sur les données à caractère personnel.

- **Le principe de finalité**

Le principe de limitation des finalités établit, d'une part, que les données à caractère personnel peuvent être traitées pour la ou les finalités prévues initialement uniquement et, d'autre part, que tout traitement ultérieur des données collectées est interdit sans un nouveau consentement de la personne concernée.

- **Le principe d’exactitude**

Le principe d'exactitude est étroitement lié à celui de transparence. Il prescrit que toutes les données à caractère personnel soient exactes et tenues à jour. Par ailleurs, il donne aux citoyens le droit de faire rectifier celles qui seraient inexactes.
Le principe de minimisation.

- **Le principe de conservation limitée des données**

Les données ne peuvent être conservées que pour une durée prédéfinie et limitée ; la finalité du traitement détermine la durée de conservation. A l'issue du traitement, les données sont soit anonymisées soit conservées pour une réutilisation ultérieure à des fins de recherche scientifique uniquement.

- **Le principe de sécurité (la confidentialité des données**

Article 385 : Principe de confidentialité et de sécurité

Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Section 3 : Profil de poste

Le DPO est donc l'interlocuteur référant de l'entreprise pour tout ce qui est lié à la gestion et à la protection des données. Il est celui qui conseille et coordonne les actions permettant d'assurer la bonne gestion des données.

En ce qui concerne la protection des données à caractère personnel. Les organisations qui traitent des données à caractère personnel de manière intensive ont besoin d'expertise afin de vérifier si toutes les règles sont respectées. Dans leur quête de la bonne expertise, ces organisations sont rapidement confrontées à la question de savoir si l'expert sélectionné doit plutôt être un juriste ou un technicien, ou les deux…

Là où un expert ayant de connaissances plutôt techniques peut répondre à la question de savoir si toutes les mesures de sécurité techniques ont été prises pour garantir un traitement sans risque des données à caractère personnel.

La question de savoir si vous devez, en tant qu'entreprise, plutôt rechercher un expert technique ou juridique dépendra également de l'expertise dont vous disposez déjà en interne.

A défaut de disposer des connaissances juridiques au sein de l'entreprise il faut recourir à une personne qui connait vraiment les deux domaines d'expertises. On peut faire aussi recours à une personne qui connait suffisamment les deux domaines d'expertises.

Quoi qu'il en soit, la protection des données est typiquement une expertise qui se trouve à la jonction entre l'aspect juridique et l'aspect TIC/technique. Pour réussir en tant que DPO, la connaissance des deux domaines est indispensable.

Par ailleurs, le délégué doit :

- Se comporter avec honnêteté, exactitude, équité et indépendance.
- Offrir uniquement les services professionnels pour lesquels il dispose de la pleine capacité d'exécution, d'informer de façon adéquate les responsables de traitement sur la nature des missions assurées ou des services proposés, y compris toute préoccupation ou risque encouru ;
- De traiter de façon confidentielle toute information acquise au cours de relations professionnelles.
- De donner priorité, dans toutes leurs actions et réflexions, à la protection des données personnelles des personnes concernées.

Section 4 : Modalités de désignation et mise en place

Que la désignation d'un délégué revête ou non un caractère obligatoire, les organismes bénéficient d'une certaine liberté dans le choix de leur délégué :

- Il n'a pas à répondre à un profil particulier (personne issue du secteur juridique, technique ou autre ; pas de certification obligatoire).
- Il peut être interne ou externe à l'organisme, à temps plein ou à temps partiel, personne physique ou morale, mutualisé ou non pour plusieurs organismes.

Mais pour que la désignation d'un DPO soit valable, elle doit nécessairement répondre à quatre conditions :

- Qualités professionnelles:

L'article 430 prévoit que le délégué soit désigné sur la base de ses qualités professionnelles, en particulier de ses connaissances spécialisées en matière de protection des données, mais également de sa capacité à accomplir les missions d'information, de conseil, de contrôle, et d'interface qui lui incombent.

- Il est à l'abri des conflits d'intérêts au regard de ses éventuelles autres activités:

• Lorsque la personne choisit pour être délégué occupe déjà une autre fonction, ou est appelée à exercer d'autres missions ou tâches au sein de l'organisme, l'organisme doit s'assurer qu'elle pourra agir en toute impartialité : le délégué ne doit pas être à la fois juge et partie.

• Il doit-être en mesure de conseiller de manière objective et ne pas être amené à contrôler ce qu'il a lui-même décidé.

• En effet, ces fonctions impliquent la plupart du temps un pouvoir décisionnaire dans la détermination des objectifs et des conditions de mise en œuvre des traitements.

• Le risque de conflit d'intérêts s'apprécie toutefois au cas par cas, en particulier au regard de la structure organisationnelle de l'organisme.

- Il bénéficie de moyens suffisants:

Le délégué doit bénéficier des moyens nécessaires à l'exercice de ses missions. Les organismes sont tenus de s'assurer que leur délégué est suffisamment impliqué et outillé.

En pratique, il s'agira de lui offrir un soutien actif et pérenne en garantissant sa visibilité et en l'associant, de façon appropriée et en temps utile, à toutes questions relatives à la protection des données personnelles :

- Information le plus en amont possible sur les projets de traitements.
- Invitation aux réunions axées sur des sujets impliquant des problématiques « Informatique et Libertés ».
- Prise en compte de ses recommandations.
- Publication de ses coordonnées à l'intention des tiers/personnes concernées, etc.

- Il a la capacité d'agir de façon indépendante dans l'accomplissement de ses missions:

L'organisme doit s'assurer de l'existence de garanties d'indépendance, à la fois au stade de la désignation du DPO et de l'exercice de sa fonction :

- Il doit faire directement rapport au niveau le plus élevé de la direction de l'organisme pour que celui-ci ait connaissance de ses avis et recommandations. Des temps et des moyens d'échanges réguliers et directs doivent ainsi être prévus.
- Il ne doit pas recevoir d'instruction dans l'exercice de ses missions de délégué que ce soit sur la manière de traiter un sujet, d'interpréter une disposition légale, d'instruire une plainte, d'analyser le résultat d'un audit, ou sur l'opportunité de consulter l'APDP.
- Aucune sanction (ex : Licenciement, frein à l'avancement de la carrière) ne peut être fondée sur l'accomplissement de ses missions. Par exemple, le délégué ne peut être relevé de ses fonctions s'il conseille au responsable de traitement d'effectuer une analyse d'impact alors que celui-ci n'est pas d'accord. En revanche, il est possible de mettre fin aux fonctions du délégué pour des raisons légitimes comme faute grave (absences injustifiées, vol, harcèlement, etc.).

Le DPO est l'interface entre l'APDP et l'organisme qu'il représente :

- Est le point focal de l'APDP auprès de son organisme
- Joue le rôle de facilitateur entre son organisme et l'APDP
- Répond à l'ensemble des demandes qu'elle pourrait émettre lors d'un contrôle sur place
- Demande l'avis de l'Autorité sur une analyse d'impact présentant un risque élevé
- Demande conseille auprès de l'Autorité sur d'éventuels traitements à mettre en œuvre.

MERCI POUR VOTRE ATTENTION