DPDP ET GESTION DES TIERS INTERVENANTS

NOVOTEL COTONOU les 19 AU 21 Décembre 2022

Par Ambroise Dj. ZINSOU

Consultant formateur indépendant
Management Télécoms & TIC et Protection
des données personnelles et de la vie privée

AGENDA

DPDP et gestion des tiers intervenants

- **Sous-traitance**
- **Communication des données**
- **Transfert de données**

INTRODUCTION

Introduction

Les sources de données personnelles sont multiples [puissances publiques, entreprises publiques et privées, personnes , voire des machines elles-mêmes]. La donnée circule, se copie, se stocke, s'agrège, se corrèle. Avec le développement récent de l'intelligence artificielle, le volume de données personnelles s'est accru de manière exponentielle rendant leur protection difficile

Ainsi, à l'heure actuelle, la donnée devient la matière première de nombreux métiers et la raison d'être de nouveaux marchés, témoignant d'une tendance généralisée qu'est l'économie guidée par les données [data driven economy].
Pour valoriser ces actifs, il est nécessaire de disposer des moyens et outils de mesures spécifiques pour traiter ces *Big Data ce que les organismes n'ont pas toujours* d'où l'obligation de mettre en œuvre l'organisation qui sied en fonction de son domaine d'invention pour la valorisation des données personnelles ainsi collectée. Avec la mondialisation qui pousse à l'externalisation des filières économiques, le recours à la sous-traitance est de plus en plus fréquent donc nécessaire, au-delà même des frontières nationales, soit pour une question de spécialisation principale dans leur domaine d'activité, de rentabilité, de planification stratégique ou même de gestion d'échéances serrées. Elle devient une option que de plus en plus d'organismes envisagent. Aussi appelée l'impartition, la sous-traitance apporte beaucoup d'avantages, mais présente des enjeux importants à connaître [les risques possibles liés à la sous-traitance]

A. SOUS-TRAITANCE

SOUS-TRAITANCE

I. Importance de la sous-traitance

L'impartition présente de nombreux avantages et permet aux entreprises de se concentrer, sur leur spécialisation principale. Cependant, tout n'est pas rose et il y a des constats importants à faire avant de rédiger un contrat de sous-traitance. La sous-traitance permet donc : **Une meilleure utilisation de la division du travail et donc de la spécialisation**.

L'entreprise pourra également se concentrer sur ses activités de recherche et développement et d'innovation en déléguant la protection en tant que responsable de traitement à ses sous-traitants.

II. Le rôle du sous-traitant en matière de traitement des données personnelles

L'une des interrogations contemporaines en matière de sous-traitance porte sur le traitement des données personnelles. Depuis plusieurs décennies déjà, la sous-traitance est un phénomène économique très développé en matière numérique car le traitement des données personnelles se prête tout particulièrement à l'externalisation du stockage des données et au *cloud computing*. Comme dans les autres secteurs, une entreprise confie le traitement de données en totalité ou en partie à une autre entreprise prestataire, le sous-traitant, ce qui permet une spécialisation des tâches et des économies d'échelle. L'enjeu en la matière est que le recours à la sous-traitance fragilise la sécurité de la relation principale entre la personne concernée et la responsable de traitement : elle créé un risque s'agissant du respect du droit des données personnelles par le sous-traitant. Pour y remédier et garantir les droits des personnes concernées, les sous-traitants deviennent des acteurs nouveaux du droit des données personnelles : ils se voient imposer des obligations spécifiques et encourent désormais une lourde responsabilité du fait du traitement des données personnelles. L'objectif est de garantir la protection des données confiées aux sous-traitants en raison du risque que leur intervention fait peser sur les données personnelles traitées. Pour limiter ce risque, il est ainsi demandé au responsable du traitement de « choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements, notamment pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité, de manière à ce que le traitement réponde aux exigences du présent Livre et garantisse la protection des droits des personnes concernées » [Art. 380.1].

Le recours à la sous-traitance ne doit pas conduire à l'affaiblissement de la protection des personnes concernées. A l'inverse, il s'agit d'assurer une meilleure répartition des obligations et des responsabilités, et corrélativement une meilleure protection des données personnelles.

III. Le sous-traitant : un nouvel acteur du code

Le livre V du code du numérique a conduit à une consécration étroite de la notion de sous-traitant ainsi qu'à la mise en place d'un régime juridique composé d'obligations à la charge du sous-traitant .

3.1. La consécration étroite de la qualité de sous-traitant

Le code du numérique définit, le sous-traitant comme « **la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement** ». Cette disposition est confortée par l'article 386. Al.1er du livre V du code.

En pratique, de nombreuses situations correspondent à cette définition : l'entreprise qui confie la gestion de données personnelles à un prestataire de services informatiques, à un prestataire intégrateur de logiciels, à une société de cybersécurité, ou encore à une entreprise de marketing pour des campagnes de prospection commerciale. Les hypothèses sont nombreuses où une entreprise va s'en remettre à une autre concernant la gestion des données personnelles. Pour autant, ces situations ne correspondent pas nécessairement à la notion de sous-traitance telle que définit par le code. En effet, le critère de la sous-traitance vise le traitement de données personnelles pour le compte d'un autre organisme « … sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu »[Art 386.4 du CDN]

L'application des dispositions du livre V impose d'identifier précisément les rôles respectifs des acteurs à travers un contrat [Art 386.5 du CDN]. Dans ce cas, le responsable de traitement est défini comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement », ce qui distingue le sous-traitant du responsable de traitement, qui ne peut définir ni les finalités ni les moyens sans être requalifié de responsable de traitement ce qui pourrait constituer un manquement au code. Les responsabilités de chacun doivent donc être réparties par le contrat dans le respect des dispositions du livre V du Code.

Par contre, si un organisme dit sous-traitant traite des données traite les données sans agir sur instructions du responsables de traitement, elle n'est pas un sous-traitant. Elle sera qualifiée d'entreprise prestataire de services et dans ces conditions assimilable à un responsable de traitements.

Comme celle de responsable de traitement, la notion de sous-traitant est donc une notion fonctionnelle qui doit correspondre à la qualification retenue par les parties dans leur contrat. Les parties disposent d'une grande liberté pour déterminer leurs responsabilités respectives dans le contrat de sous-traitance, mais encore faut-il

que la qualification contractuelle coïncide bien avec la réalité de leurs rôles respectifs.

3.2. Les obligations imposées aux sous-traitants

Des obligations nouvelles sont imposées au sous-traitant qui sont largement similaires à celles relevant du responsable de traitement. Le livre V du code fixe en effet un ensemble d'obligations aussi bien aux responsables de traitements qu'aux sous-traitants susceptibles d'intervenir dans les opérations de traitement. Selon l'article 435. Al. 1er et 2 du livre 5 du code , chaque sous-traitant doit tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, que le traitement est susceptible de comporter un risque pour les droits et des libertés des personnes, que les traitements sont réguliers ou qu'ils portent sur des catégories spéciales de données ou de données de condamnations ou d'infractions. Le registre tenu sous forme écrite doit être mis à disposition de l'autorité de contrôle sur demande. Le registre comporte l'identification de chaque responsable de traitement pour lequel le sous-traitant agit, les catégories de traitement effectuées pour le compte de chaque responsable, les transferts transfrontières de données, et la description générale des mesures de sécurité techniques et organisationnelles adoptées visées à l'article 426 du livre V du code. En effet, le sous-traitant est visé à l'égal du responsable de traitement par l'article 426 du livre V du code relatif à la sécurité des données à caractère personnel : ainsi, le sous-traitant doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque. À l'image du responsable de traitement, le sous-traitant peut être tenu de désigner un délégué à la protection des données dans les mêmes conditions visées par l'article 430 du livre V du code. Une obligation de coopération avec l'autorité de contrôle est également imposée au sous-traitant à l'égal du responsable de traitement

S'agissant de sa relation avec le responsable de traitement, le sous-traitant est soumis à des obligations spéciales décrites dans l'article 386.1 du livre V. Il est à nouveau tenu de mettre en œuvre des garanties suffisantes quant à la mise en œuvre « de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits des personnes concernées ». Le sous-traitant pourra faire appel à un sous-traitant de second rang avec l'autorisation écrite préalable du responsable de traitement. Cet autre sous-traitant est soumis aux mêmes obligations que celles du sous-traitant de premier rang. Mais en cas de non-respect de la protection des données, « (…) le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations ». En retenant la responsabilité du sous-traitant de premier rang pour un manquement réalisé par le sous-traitant de second rang, on impose que le recours à la seconde sous-traitance soit maîtrisé par le premier sous-traitant.

Le nouveau régime prévoit de manière obligatoire des dispositions spéciales au sein du contrat liant le sous-traitant et le donneur d'ordre. Une contractualisation est désormais requise par contrat ou un autre acte juridique, sous forme écrite y compris en format électronique. [Art. 386.5 du CDN]. Ce contrat doit prévoir une liste non exhaustive de mentions telles : l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement, des obligations spécifiques en matière de confidentialité, de sécurité [Art. 426 du CDN], de conseil auprès de leurs clients, d'analyse d'impact pour les traitements à risque [429.1 du CDN], réponses à l'exercice des droits des usagers [Art 426 al 4 et 6 du CDN], prévoir le sort des données traitées : ainsi, le sous-traitant devra supprimer ou renvoyer les données, et détruire les copies existantes selon les instructions du responsable de traitement

IV. Le sous-traitant : un acteur responsable

Des changements importants concernent la responsabilité et la sanction du sous-traitant. Le règlement consacre une responsabilité autonome du sous-traitant , et partant, de nouvelles règles en matière de responsabilité et de sanctions administratives encourues par le sous-traitant. Toutefois, le sous-traitant peut faire l'objet d'une requalification lorsque son rôle ne correspond pas à la notion de sous-traitance étroitement telle que défini par le code.

4.1. <u>Le principe de la responsabilité directe et personnelle du sous-traitant</u>

Jusqu'à l'entrée en vigueur du Code, le sous-traitant ne pouvait être tenu pour responsable d'un manquement à une disposition relative à la protection des données personnelles face à une autorité de contrôle. Il n'existait qu'un seul responsable, le responsable de traitement.

Avec l'entrée en vigueur du code en 2018, en cas de violation du règlement, les principes directeurs du droit à réparation et de la responsabilité fixés par l'article 451 du code du RGPD visent à la fois le responsable de traitement et le sous-traitant. Le principe de la responsabilité du sous-traitant est affirmé dès le début de l'article : toute personne ayant subi un dommage matériel ou moral du fait d'une violation des dispositions du live 5 peut obtenir la réparation de son préjudice de la part du responsable de traitement ou du sous-traitant. Désormais, la réparation peut être obtenue aussi du sous-traitant. Toutefois, cette responsabilité n'est pas encourue de manière automatique : alors que la responsabilité du responsable de traitement est engagée pour tout dommage causé par le traitement qui constitue une violation des dispositions du code, la mise en œuvre de la responsabilité propre au sous-traitant est conditionnée par l'article 451.2. du livre 5 à deux cas : d'une part, la violation des obligations prévues spécifiquement à l'égard des sous-traitants, et d'autre part la violation

des instructions licites du responsable du traitement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que dans ces deux cas.

Que ce soit celle du responsable du traitement ou celle du sous-traitant, la mise en jeu de la responsabilité nécessite l'imputabilité personnelle d'un fait ayant provoqué le dommage et il ne peut y avoir de responsabilité du fait d'autrui. Aussi, en l'absence d'imputation personnelle du fait ayant provoqué le dommage, chaque acteur bénéficie d'une exonération de responsabilité à condition d'en rapporter la preuve en vertu de l'article 451. 3. du Code.

En outre, le sous-traitant et le responsable de traitement peuvent être solidairement responsables de l'indemnisation du préjudice subi par les personnes concernées : dans ce cas, chacun peut être tenu de réparer la totalité du dommage à la victime, et peut ensuite réclamer aux autres responsables la part de réparation correspondant à leur part de responsabilité dans le dommage [Art. 451. 4 et 5 du CDN]. Cette responsabilité solidaire permet de garantir à la victime une réparation effective.

4.2. Le risque d'une requalification en responsable de traitement

La notion de sous-traitance retenue par le Code est étroitement délimitée, ce qui crée des incertitudes concernant la qualification juridique : dans de nombreuses situations, le régime de la sous-traitance apparait trop étriqué pour qualifier la situation dans laquelle le sous-traitant excède ce rôle de simple exécutant qui agit sur les instructions du responsable de traitement.

De fait, si le sous-traitant dépasse le rôle qui lui a été assigné par contrat, une requalification est possible en responsable de traitement avec responsabilité conjointe. Cette situation est fréquente en pratique, notamment lorsque la relation entre le donneur d'ordre et le sous-traitant est déséquilibrée : le sous-traitant peut être en position de force en raison de l'émergence de prestataires numériques puissants qui proposent des offres standardisées. Dans ce cas, il serait difficile au responsable de traitement d'imposer à leurs sous-traitants les prescriptions du Code. Si le responsable de traitement ne peut négocier avec le sous-traitant et lui imposer ses instructions, ce dernier peut se voir attribuer la qualité de responsable de traitement. Dans de telles situations la responsabilité conjointe peut concerner des acteurs que l'on aurait jusque-là qualifié de sous-traitants [Art. 388 du CDN].

Le code consacre expressément la co-responsabilité des acteurs et impose désormais aux responsables conjoints d'un traitement de conclure un accord définissant leurs obligations et précisant leurs rôles respectifs.

V. Les avantages de la Sous-traitance

La sous-traitance permet :

- Une plus grande maîtrise de la qualité ;
- des coûts et des délais de traitement maitrisés ;
- Une meilleure réactivité face aux flux important de données du fait de l'augmentation de la demande du marché ;
- Une réduction des risques de défaillances techniques.

VI. types de Sous-traitance

Classiquement, on distingue trois types de sous-traitance :

- la **sous-traitance** de spécialité [le donneur d'ordres fait appel à un « spécialiste » disposant des équipements, des matériels et de la compétence adaptés à ses besoins, parce qu'il ne peut ou ne souhaite pas s'en doter, pour des raisons relevant de sa stratégie propre ;

- **la sous-traitance de capacité.**[**le** donneur d'ordres, équipé lui-même pour exécuter un traitement, a recours à un **sous-traitant**: soit occasionnellement, en raison d'un pic momentané d'activités ou d'un incident technique; soit parce que désireux de conserver en interne une capacité de traitement propre.] ;

- **La sous-traitance de marché** : c'est le cas où une entreprise fait appel à une autre pour remplir un marché conclu entre elle et un maître d'ouvrage

VII. Les obligations et la responsabilité du sous-traitant

En tant que sous-traitant, tout organisme a des obligations et peut voir sa responsabilité engagée. Ces obligations sont notamment les suivantes :

- Une obligation de transparence et de traçabilité : établir un contrat avec le client précisant les obligations du prestataire, recenser les instructions données par le client, mettre à disposition du client les informations nécessaires démontrant le respect des obligations de sous-traitant, demander l'autorisation de recourir à un sous-traitant, établir un registre des traitements ; [Art 426 al 4 et 6 du CDN ;]

- La prise en compte des principes de protection by design et de protection by default : pour en savoir plus sur ces principes [art. 424 du CDN] ;

- Obligation de désigner les catégories de personnes, devant avoir accès aux données à caractère personnel avec une description précise de leur fonction par rapport au traitement des données visées dont la liste devra être communiquée à l'Autorité via le RT [Art 402.1 et 2 du CDN] ;

- Une obligation de garantir la sécurité des données traitées : obligation de garantir la confidentialité des données, obligation de notifier toute violation des données au responsable de traitement, obligation de prendre les mesures nécessaires pour garantir la sécurité des données, éventuellement désigner un DPDP/DPO [Art 386.1] ;

- L'obligation de garantir la sécurité des données à caractère personnel, par la mise en oeuvre des mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, l'interception notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite [Art 426 al premier du CDN] ;

- sous- traitant a l'obligation de veiller au respect de ces mesures de sécurité [la pseudonymisation et le chiffrement ; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;] [Art 426.1 à4] ;

- Une obligation d'alerte, d'assistance et de conseil : aider le responsable de traitement dans la gestion des demandes des personnes concernées, l'informer sur les risques éventuellement engendrés par une instruction, et plus généralement aider le client à respecter ses obligations en matière de protection des données.

Cette liste non exhaustive d'obligations conduit à la possibilité d'engager la responsabilité du sous-traitant si celui-ci ne démontre pas le respect de ses obligations. Il faut donc faire preuve de vigilance lors de la réalisation de tout traitement de données en tant que sous-traitant.

B. COMMUNICATION DE DONNEES

COMMUNICATION DE DONNEES

Deux concepts sont retenus par le code du numérique. L'échange de données entre acteurs dans l'espace UEMOA est considéré comme une communication de données intra muros . Hors espace UEMOA, la communication des données est traitée comme un transfert de données personnelles vers une Etat tiers ?

I. Communication dans l'espace UEMOA

1.1. Demande d'information

La communication des données de la personne concernées à des tiers ou non dans cette espace peut se faire d'un pays à un autre sans une contrainte dès lors que les dispositions de protection des données personnelles sont presque à l'identique et respectées et que tous les pays de l'espace sont supposés avoir harmonisé leur lois et disposer d'une autorité de contrôle.

Au Bénin, en application des dispositions du livre V du code du numérique, toute personne concernée par un traitement peut demander à un organisme traitant ses données, la communication de celles-ci qu'il détient sur elle et en obtenir une copie.[Art. 437.2 du CDN]. En effet, l'exercice du droit d'accès permet à une personne de savoir si des données qui la concernent sont traitées puis d'en obtenir, « la communication sous forme intelligible des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci » [Art.437.2 du CDN]

En outre, le droit à la portabilité donne également la possibilité à la personne concernée de recevoir « communication des données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine… » [Art 438. Al 1er du CDN]

L'organisme auprès duquel une personne souhaite exercer son droit d'accès doit également être en mesure de lui fournir divers renseignements, par exemple les objectifs poursuivis par l'utilisation des données, les catégories de données traitées, les autres organismes ayant obtenu la communication des données.

1.2. Communication de données personnelles aux tiers

i. Tiers personne

Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du

traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

S'agissant de la communication des données personnelles aux tiers, elle est subordonnée au consentement de la personne concernée sauf dans les cas d'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, de l'exécution d'un contrat auquel la personne concernée est partie ou de l'exécution de mesures précontractuelles prises à sa demande , de l'exécution d'un contrat auquel la personne concernée est partie ou de mesures précontractuelles prises à sa demande . [Art 389. 1 à 4]

La personne concernée a le droit de s'opposer à la communication de ses données à des tiers dans certains cas [art 440. Al 2 du CDN]. Selon la disposition, il doit en être informé.

Procéder à une collecte déloyale de données à caractère personnel ; communiquer à un tiers non autorisé des données à caractère personnel ; procéder à la collecte de données sensibles, de données relatives à des infractions ou à un numéro national d'identification sans respecter les conditions légales ; procéder à la collecte ou à l'utilisation de données à caractère personnel ayant pour conséquence de provoquer une atteinte grave aux droits fondamentaux ou à l'intimité de la vie privée physique la personne concernée sont considérés comme des manquements graves punis par la loi ; [Art 453. 1 à 4 du CDN]

ii. Les **tiers autorisés**

Les tiers autorisées sont des autorités et des organismes habilités, par des dispositions législatives, à ordonner à un responsable de traitement le transfert de documents ou de renseignements contenant des données à caractère personnel de personnes déterminées.

Pour répondre valablement à une demande de communication de données à caractère personnel de la part d'un tiers autorisé, le responsable de traitement doit procéder à trois vérifications :

- la demande provient d'un tiers autorisé ;
- la source et le périmètre de la demande ;
- la sécurisation de la communication.

La mise en œuvre de cette démarche permet à chaque responsable de traitement d'assurer la sécurité des données à caractère personnel, conformément aux exigences du code

1ère vérification : l'origine, de « la demande d'un tiers autorisé »

À titre liminaire, une demande de tiers autorisé peut prendre toute **forme**, sauf si le texte en cause en prévoit une spécifiquement.
Si la demande mentionne une disposition légale ou réglementaire, le responsable de traitement doit la vérifier.

S'il ne le sait pas, le responsable de traitement doit demander au tiers autorisé la référence légale pour procéder à cette vérification.

2ème vérification : la source et le périmètre de la demande

Avant d'accéder à la demande, une double vérification, pratique et juridique, est nécessaire :

- La vérification pratique a pour objet de s'assurer que la demande provient bien de l'autorité ou de l'organisme public mentionné. Elle permet d'éviter les fraudes.
- Quant à la vérification juridique, elle vise à contrôler que l'acteur émetteur est autorisé à exiger la communication des informations demandées.

En premier lieu, afin de lever un éventuel doute concernant le tiers autorisé, plusieurs possibilités existent comme :

- effectuer un contre-appel en utilisant le numéro de contact diffusé par l'administration ;

- vérifier que l'adresse postale communiquée correspond à celle diffusée par le tiers autorisé sur son site web s'il y a lieu ;

- vérifier que le nom de domaine de l'adresse de courrier électronique utilisée correspond à celui diffusé par le tiers autorisé ;

- recueillir toute information identifiant la personne se présentant dans les locaux aux fins de vérifier qu'elle appartient à l'organisme en question.

En second lieu, le responsable de traitement doit s'assurer du périmètre des données à caractère personnel à communiquer. Les informations qui seront transmises doivent effectivement être visées par les dispositions invoquées par le tiers autorisé. En outre, la transmission ne doit pas contenir plus de données à

caractère personnel que celles demandées. Cette vérification permet de respecter le principe de minimisation énoncé à l'article 385.4 du code.

La communication des données à caractère personnel à des tiers autorisés pose par ailleurs la question du respect du secret professionnel. Celui-ci doit être opposé par le responsable de traitement à une demande provenant d'un tiers autorisé uniquement lorsqu'aucune disposition ne prévoit la levée d'un ou de plusieurs secrets professionnels.

Le responsable de traitement doit donc vérifier que les deux conditions suivantes sont réunies avant toute communication de données à caractère personnel :

- la demande de communication de données à caractère personnel est-elle couverte par un secret professionnel ?

- si tel est le cas, la demande de communication provient-elle d'un organisme bénéficiant d'une disposition législative prévoyant la levée du secret professionnel concerné ?

3ème vérification : la sécurisation de la communication

Chaque responsable de traitement doit déterminer un **canal de communication** des informations demandées entre lui et le tiers autorisé, et veiller à ce que les modalités de cette transmission en assurent la sécurité, notamment par un procédé de chiffrement, hachage, etc.

.

Le refus de communication des données à la demande d'un tiers autorisé

Il est possible de refuser d'accéder à une telle demande, mais cela peut aboutir à l'engagement de la responsabilité du responsable de traitement.

Recommandation : Il est recommandé de documenter la gestion des demandes émanant de « ***tiers autorisés*** » et de diffuser cette **documentation** auprès des personnes en charge des demandes. Elle peut indiquer les premières actions à faire par tout agent à la réception d'une demande, faire mention de la nécessité d'une désignation d'un référent chargé de la prise en compte des demandes, comporter des éléments de sensibilisation des agents et des salariés, ou bien encore faire état des outils permettant de sécuriser la communication de données à caractère personnel (ex : outil de chiffrement, politique de mot de passe, etc.).

C. TRANSFERT DE DONNEES

TRANSFERT DE DONNEES

I. Principe général applicable aux transferts

Un transfert de données à caractère personnel destinées à faire l'objet d'un traitement, vers un pays tiers c'est-à-dire hors UEMOA ou à une organisation internationale, ne peut se faire que si, les conditions définies dans le livre V du code sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données personnelles au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions de sécurité prévues par le livre V du Code du numérique doivent être respectées de manière à ce que le niveau de protection des personnes concernées ne soit pas compromis.

II. Transferts fondés sur autorisation de l'autorité de contrôle

Les transferts de données personnelles vers un pays tiers ou à une organisation internationale ne peuvent avoir lieu que lorsque l'Autorité de protection des données personnelles a constaté que les pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ces pays tiers, ou l'organisation internationale en question assurent un niveau de protection adéquat en application des dispositions de l'article 391 du code du numérique. De tels transferts nécessitent des autorisations spécifiques qui doivent être délivrées par l'autorité.

Lorsqu'elle évalue le caractère adéquat du niveau de protection, l'Autorité tient compte, en particulier, des éléments suivants :

a) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le 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;

b) 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; et

c) 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.

L'Autorité, après avoir évalué le caractère adéquat du niveau de protection, peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat. L' autorisation prévoit un mécanisme d'examen périodique. L'Autorité suit, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales .

Lorsque les informations disponibles révèlent, en particulier à l'issue de l'examen qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat, l'autorité pour être amené à abroger, modifier ou suspendre l'autorisation.

III. Transferts moyennant des garanties appropriées

le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

Les garanties appropriées peuvent être fournies par:

a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ;

b) des règles d'entreprise contraignantes ;

c) des clauses types de protection des données adoptées par l'autorité ;

d) un code de conduite approuvé assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; ou

e) un mécanisme de certification approuvé, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays

tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

IV. Règles d'entreprise contraignantes

L'autorité de contrôle compétente approuve des règles d'entreprise contraignantes à condition que:

a) ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ;

b) elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel ;

Les règles d'entreprise contraignantes doivent préciser au moins :

c) la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités ;

d) les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question;

e) leur nature juridiquement contraignante, tant interne qu'externe;

f) l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes;

g) les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes;

h) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute

violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'UEMOA; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause;

i) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) du présent paragraphe sont fournies aux personnes concernées,

j) les missions de tout délégué à la protection des données, désigné conformément à l'article 430 du CDN, ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations ;

k) les procédures de réclamation ;

l) les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou à l'entité visée au point h) et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, et devraient être mis à la disposition de l'autorité de contrôle compétente sur demande ;

m) les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle ;

n) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures visés au point j);

o) les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes; et

p) la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

L'Autorité peut, pour les règles d'entreprise contraignantes, préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent.

V. Exception

Conformément aux dispositions de l'article 392 du Code, Un transfert ou une catégorie de transferts de données à caractère personnel vers un État tiers ou une organisation internationale et n'assurant pas un niveau de protection adéquat, peut être effectué dans l'une des conditions suivantes:

a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence d'autorisation formelle de l'APDP et l'assurance de garanties appropriées de sécurité;

b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;

c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;

d) le transfert est nécessaire pour des motifs importants d'intérêt public ;

e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;

f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

g) le transfert a lieu au départ d'un registre destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation sont remplies dans le cas particulier.

Sans préjudice des dispositions de cet article, le Conseil des Ministres peut par décret et après avis conforme de l'Autorité, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un État tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat et

suffisant, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

VI. Coopération internationale dans le domaine de la protection des données à caractère personnel

En application des dispositions de l'article 483.25, l'autorité de contrôle prend, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour:

a) élaborer des mécanismes de coopération internationale destinés à faciliter l'application effective de la législation relative à la protection des données à caractère personnel;

b) se prêter mutuellement assistance sur le plan international dans l'application de la législation relative à la protection des données à caractère personnel, y compris par la notification, la transmission des réclamations, l'entraide pour les enquêtes et l'échange d'informations, sous réserve de garanties appropriées pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux ;

c) associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération internationale dans le domaine de l'application de la législation relative à la protection des données à caractère personnel ;

d) favoriser l'échange et la documentation de la législation et des pratiques en matière de protection des données à caractère personnel, y compris en ce qui concerne les conflits de compétence avec des pays tiers.

JE VOUS REMERCIE