LES OBLIGATIONS DES RESPONSABLES DE TRAITEMENT

JURISTE

Alao Olayodé ADJASSA

Juriste d'affaires et du numérique, ingénieur contractuel, conseil en investissements, DPO Externe

Président du cabinet 360 Conseils SAS

+229 67 96 72 72 - 67 10 30 10 infos@360conseils.com www.360conseils.com

SOMMAIRE

INTRODUCTION

Au nombre des acteurs de la protection des données à caractère personnel, le responsable de traitement est l'un des acteurs majeurs. Le CDN le définit comme 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 (article 1).

En tant que tel, le responsable de traitement est, avec ses éventuels sous-traitants et l'Autorité, le principal agent de protection des données à caractère personnel. Le CDN le traite à sa juste valeur en mettant à sa charge un contingent d'obligations qui le responsabilise.

Avant d'aborder les obligations spécifiques, évoquons **trois (03) points non moins importants**.

LA FORMATION DU PERSONNEL

Cette obligation vise notamment à informer sur les fondamentaux relatifs à la protection des données à caractère personnel de sorte à ce que chaque salarié comprenne les notions de protection et se sente concerné.

L'information doit se faire continuellement.

L'obligation peut être satisfaite sous forme :

- **de réunions de sensibilisation dont il faudra conserver les preuves,**
- **de campagne de communication visuelle par affichages, dépliants, pop-ups sur l'intranet de l'organisme, courtes vidéos thématiques etc.**

Tout moyen est bon pour faciliter l'assimilation des messages en termes de protection des données et obtenir une large adhésion des différents acteurs.

Les nouveaux arrivants pourraient même être invités à une formation initiale sur le sujet dans leur parcours d'intégration.

Enfin, il faut garder à l'esprit, que ces séances de sensibilisations ou de formations seraient plus faciles à prouver si elles sont sanctionnées par des attestations de suivi.

RESPONSABILITÉ CONJOINTE DU TRAITEMENT

Lorsque deux responsables du traitement ou plus déterminent conjointement et les moyens du traitement, ils sont les responsables conjoints du traitement.
Ils définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du Code du Numérique, par voie d'accord entre eux.
Un point de contact pour les personnes concernées peut être désigné dans l'accord.

L'accord doit refléter les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées.

Les grandes lignes de l'accord sont mises à la disposition de la personne concernée. Indépendamment des termes de l'accord visé à l'alinéa 1, la personne concernée peut exercer les droits que lui confèrent les dispositions du code du numérique à l'égard de et contre chacun des responsables du traitement (art 388 du CDN).

LE CHOIX DU SOUS-TRAITANT ET PRÉCISION DE LA RELATION CONTRACTUELLE

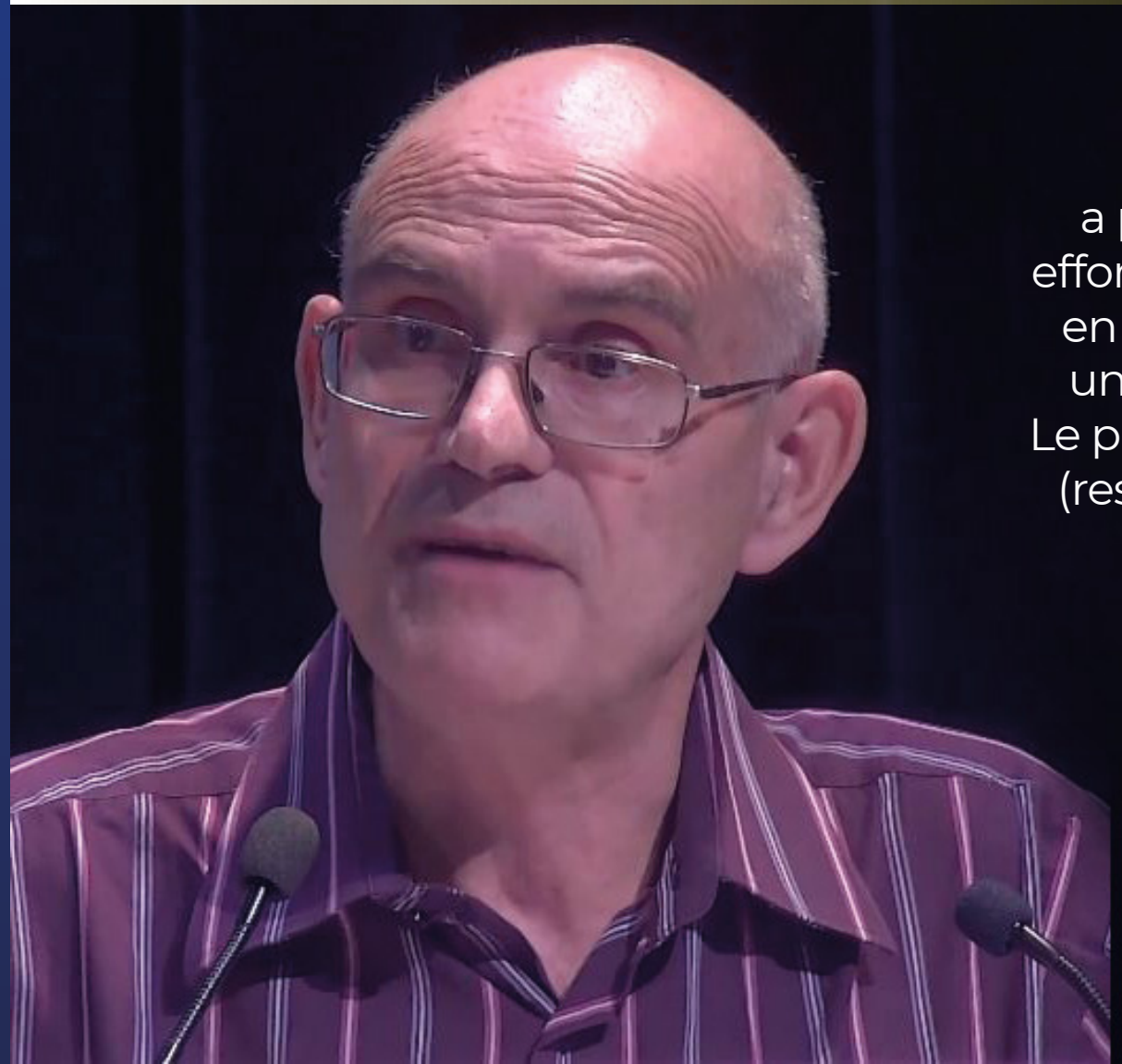
Lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en République du Bénin, doit (art 386 du CDN) :

- Choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements ;
- Veiller au respect des mesures du point ci-dessus, notamment par la stipulation de mentions spécifiques dans les contrats passés avec des sous-traitants ;
- Fixer dans le contrat, la responsabilité du sous-traitant à l'égard du responsable du traitement et les obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données ;
- Convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu ;
- Consigner par écrit ou sur un support électronique les éléments du contrat visés dans le présent article.

Concrètement, le CDN a donc posé en premier lieu, une obligation de responsabilité pour traduire littéralement le terme anglais d’accountablity.

A

L'OBLIGATION DE REDEVABILITE (L'ACCOUNTABILITY)



Yvon Pesqueux a procédé à un séduisant effort d'élaboration de bout en bout de la notion, dans une étude parue en 2020, Le principe d'accountability (responsabilité), Post-Print halshs-02898174, HAL.

A

L’OBLIGATION DE REDEVABILITE (L’ACCOUNTABILITY)

Pour lui, « avec ce principe, il se passe en effet quelque chose au-delà du plat « rendre compte » ou du terme de « responsabilité » qui consacre sa traduction en français dans les « jargons » internationaux.

La première idée qu'il comporte est celle de la comptabilité au sens de compter, mais dégagée ici de son objet patrimonial et financier. Il s'agit ici de mesurer ce qui compte.

Il s'agit ensuite d'être en mesure d'exercer le pouvoir lié au fait de savoir.

La troisième idée est celle de processus, donc de responsabilisation plus que de responsabilité et c'est là qu'il est question de redevabilité.
La quatrième idée est celle de rendre compte, de raconter en quelque sorte.

Yvon Pesqueux

A

L'OBLIGATION DE REDEVABILITE (L'ACCOUNTABILITY)

Dans une tournure quelque peu foucaldienne, on pourrait dire que l'accountability recouvre le pouvoir de savoir et le pouvoir du savoir et l'on retrouve bien ici aussi la perspective de la responsabilité. On pourrait, à ce titre, faire de ce principe une matérialisation du principe de transparence. La substance conventionnelle de ce dernier entache d'autant plus la qualité principielle du principe d'accountability qui est plutôt de l'ordre de la reddition. Il présente par contre l'intérêt de légitimer le recours au contrôle externe et de fonder d'autant les juteuses prestations de l'audit qui y sont associées.

Yvon Pesqueux

La notion bénéficie de la dimension symbolique de la référence à un Dieu qui demande de rendre des comptes, au moment de la mort, de ce que l'on a fait de sa vie. Il entre en effet de composition avec le principe de transparence puisqu'il s'agit, dans les deux cas, d'être visible, le principe de transparence recouvrant l'idée de processus de mise en visibilité et le principe d'accountability l'idée de se mettre sous le regard des autres. »

Yvon Pesqueux

Inversement du paradigme de contrôle de cnformité **=** **accountability** **=** **se comporter en « bon père de famille »** en droit civil.

A

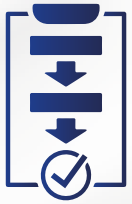
L'OBLIGATION DE REDEVABILITE (L'ACCOUNTABILITY)

Dans le CDN, la notion prend siège dans les articles 387 CDN et se dispersent dans plusieurs autres obligations mis à la charge des responsables de traitements.

2- DÉCLINAISON DU PRINCIPE

Leadership et supervision

Evaluation des risques



Politiques et procédures

Transparence

Formation et sensibilisation

Suivi et évaluation des mesures déployées

Réponse et application des règles

Documentation

Pour donner bonne application au principe de redevabilité, certaines obligations ont été expressément codifiées.

La satisfaction à cette obligation doit se démontrer d'abord à l'égard des personnes.

B

LES OBLIGATIONS A L'EGARD DES PERSONNES

1- LES MENTIONS D'INFORMATIONS

Les articles 415 et 416 du CDN énumèrent les informations à communiquer en cas de collecte directe auprès de la personne concernée et en cas de collecte indirecte.

L'obligation d'information peut être satisfaite au moment du recueil de consentement.

En pratique, cette obligation reçoit diverses applications. En général, il faudra afficher les informations ci-après :

- Mentions légales : qui êtes-vous ?
  (Footer du site, de la newsletter, du formulaire papier etc.)

- Recueil du consentement : allez-vous recueillir mes données ? Lesquelles ? Pourquoi ? Allez-vous les garder ? Pendant combien de temps ? Pourrais-je avoir accès à ces dernières ? Pourrais-je les modifier ? Si je consens maintenant, pourrais-je me rétracter plus tard ? Comment ? etc.
  (Pop-up sur la landing page du site, pop-up persistant sur tout le site, offrir la possibilité d'accepter ou de refuser sans perdre l'usage du site, macaron en cas de vidéosurveillance etc.)

B

LES OBLIGATIONS A L'EGARD DES PERSONNES

- Politique de confidentialité : les données que je vous communique sont-elles protégées ? comment ? que se passe-t-il si elles fuitent ? (Footer du site, de la newsletter, du formulaire papier etc.)

L'Autorité a également publié sur son site www.apdp.bj des modèles de recueil de consentement conformément à l'article 389 CDN qui permettent de satisfaire à l'obligation d'information en cas de traitement manuel et de traitement automatisé.

Pour les cas de traitement où il n'existe pas encore de modèles, il faudra veiller à ce que la formule adoptée reprenne à tout le moins les informations présentes sur les modèles existants de l'Autorité.

De même, il est possible de s'inspirer des modèles de mentions d'information publiés en environnement RGPD au regard des convergences du règlement avec le CDN.

B

LES OBLIGATIONS A L'EGARD DES PERSONNES

2- LES OBLIGATIONS DE NOTIFICATION

En cas de violation de données subie, le RT est tenu de notifier l'incident aux personnes concernées sauf dans certaines conditions.

La notification doit se faire sans délai à chacune des personnes concernées. Mais au cas où elle exigerait « des efforts disproportionnés », le RT pourrait procéder à une communication publique par le biais des canaux de communication traditionnels.

Toutefois, la communication publique est un recours ultime. Parce que les l'attaquant peut se servir d'une telle communication, la décision de faire une communication publique doit s'étudier et ne se prendre qu'avec précautions.

3- L'OBLIGATION DE RÉPONSE AUX DEMANDES D'EXERCICE DE DROIT

Le RT est tenu de répondre à une demande d'exercice de droit.

B

LES OBLIGATIONS A L'EGARD DES PERSONNES

Traitement de la demande

- Vérification de l'identité du demandeur
- Réponse dans le délai imparti

  - Droit d'accès et de droit à l'oubli = (30) jours + 30 jours à compter de la réception si demandeur informée des motifs du rallonge
  - Droit d'opposition = (30) jours à compter de la réception
  - Droit de rectification = (45) jours à compter de la réception
  - Sans suite = (30) jours à compter de la réception avec justification et renvoi vers l'APDP

- Vérification de l'opportunité de la réponse
  Pas d'obligation de réponse si :

  - Dispenses légales
  - Exercice du droit de refus
  - Non-paiement des frais d'accès
  - Exception de portabilité
  - Report de communication des données
  - Interdiction d'exercice du droit à l'oubli

B

LES OBLIGATIONS A L'EGARD DES PERSONNES

- Décider de la forme de la réponse : orale, écrite, par voie électronique

la réponse soit concise, transparente, compréhensible et aisément accessible, libellée en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant… (Article 418).

Choisir un mode de transmission sécurisée

LES OBLIGATIONS A L'EGARD DE L'AUTORITE

1- L'OBLIGATION DE TENUE DU REGISTRE DE TRAITEMENT

Principe

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.
Le responsable du traitement, et le cas échéant, son représentant met le registre à la disposition de l'Autorité sur demande.

En outre, conformément à l'article 387 dernier alinéa, le RT est tenu de présenter un rapport annuel de traitement pour démontrer à l'Autorité que son activité de traitement est conforme aux prescriptions du CDN.

Contenu et forme

Le registre comporte toutes les informations suivantes (art 435) :

- 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 ;
- Les finalités du traitement ;
- Une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- 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 ;

LES OBLIGATIONS A L'EGARD DE L'AUTORITE

- 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 ;
- Les délais prévus pour l'effacement des différentes catégories de données ;
- Une description générale des mesures de sécurité techniques et organisationnelles.

Pour éclairer la pratique, l'Autorité a publié sur son site www.apdp.bj , un modèle de registre qui peut être personnalisé par les RT ou servir de point de repère.

Pareillement, un guide de rédaction du rapport annuel a été publié sur le même site afin d'harmoniser les pratiques qui jusqu'ici étaient très peu renseignées.

Exception

Les petites et moyennes entreprises sont dispensées de l'obligation de tenir un registre de traitement sauf si le traitement qu'elles effectuent :

- Est susceptible de comporter un risque pour les droits et les libertés des personnes concernées ;
- N'est pas occasionnel, comme le serait un traitement effectué pour l'organisation d'un évènement ;

Pour déterminer si un organisme est considéré comme une petite et moyenne entreprise aux termes de cet article, référence pourra être faite aux dispositions du Code Général des Impôts qui procèdent à une catégorisation des entreprises.

LES OBLIGATIONS A L'EGARD DE L'AUTORITE

2- L'OBLIGATION DE SÉCURITÉ DES DCP

Prescriptions de l'article 426

Le responsable du traitement doit 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.

Cela peut se traduire par l'utilisation :

- De la pseudonymisation et du chiffrement des données à caractère personnel
- 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 les délais appropriés en cas d'incident physique ou technique ;
- D'une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

LES OBLIGATIONS A L'EGARD DE L'AUTORITE

De la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)

Le 28 octobre 2021 a vu l'adoption du décret portant **Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE)** par le Conseil des ministres sur proposition de l'ANSSI.

Cette politique est « **le support de base pour la mise en œuvre des mesures techniques, organisationnelles et physiques, par les structures de l'Etat, afin de protéger leurs systèmes d'information respectifs. ».**

L'obligation de sécurité des DCP peut être satisfaite en s'inspirant, pour les entreprises du secteur privé, ou en se conformant, pour les organismes publics, de la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE).

Le document de la politique est téléchargeable sur le site **www.anssi.bj.**

LES OBLIGATIONS A L'EGARD DE L'AUTORITE

3- L'OBLIGATION DE NOTIFICATION DES VIOLATIONS

Principe

Le CDN oblige le responsable du traitement à notifier, sans délai, à l'Autorité et à la personne concernée toute rupture de la sécurité ayant affecté les données à caractère personnel de la personne concernée (CDN, art 427 al 1er).

La notification du responsable du traitement doit contenir les mêmes informations que dans le cas d'une communication à la personne concernée.

Pour éclairer les usages, l'Autorité a mis en ligne sur son site **www.apdp.bj** un formulaire de signalement qui spécifie plus clairement les informations à transmettre.

Bonnes pratiques

Il est recommandé qu'une une procédure de notification de violation des données soit rédigée. Mathias Avocats, cabinet français spécialisé en protection des DCP a proposé les étapes clés suivante à détailler dans une telle procédure.

1. **Prévoir un système interne de signalement**
2. **Prévoir une investigation**
3. **Prévoir la mise en œuvre de mesures correctrices**
4. **Prévoir une phase d'évaluation des impacts**
5. **Prévoir les modalités de notification**

LES OBLIGATIONS DE DILIGENCES PREALABLES

Principe

Selon le RT et selon type de traitement que le RT compte mettre en œuvre, il est tenu soit de faire une déclaration préalable (1), soit de demander une autorisation (2) soit de solliciter un avis (2) auprès de l'Autorité de Protection des Données à caractère Personnel -APDP.

1- DÉCLARATION PRÉALABLE

Aux termes de l'article 405 CDN, une déclaration préalable est requise pour le « les traitements automatisés ou non automatisés exécutés par des organismes publics ou privés et comportant des données à caractère personnel ».

2- AUTORISATIONS

Selon l'article 407 CDN une demande d'autorisation doit être présentée par le responsable du traitement ou son représentant à l'APDP préalablement au traitement dans les cas suivants :

- Traitements déterminés par l'APDP ;
- Données sensibles et DCP aux fins de journalisme et d'expression littéraire et artistique ;
- Actes d'identité tels que l'ANIP, l'IFU, le passeport etc. ;

LES OBLIGATIONS DE DILIGENCES PREALABLES

- Données biométriques ;
- Traitements aux fins historiques, statistiques et scientifiques ;
- Interconnexion de fichiers ;
- Transferts de données hors CEDEAO ;
- Traitements automatisés relatifs aux difficultés sociales des personnes.

3- AVIS

Selon l'article 411 CDN, « ... Les traitements des données à caractère personnel opérés pour le compte de l'État, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont autorisés par décret pris en Conseil des ministres après avis motivé de l'Autorité.

Ces traitements portent sur :

a. La sûreté de l'État, la défense ou la sécurité publique ;

b. La prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

c. Le recensement de la population ;

d. Les données à caractère personnel faisant apparaître, directement

LES OBLIGATIONS DE DILIGENCES PREALABLES

3- AVIS

ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;

e. Le traitement de salaires, pensions, impôts, taxes et autres liquidations... »

4- EXCEPTIONS ET DISPENSES

Dans le souci d'alléger aux RT l'obligation de déclaration notamment, le CDN renonce à la déclaration préalable :

- En présence de données courantes, sous réserve du respect des normes de l'APDP ;
- En l'absence de risques d'atteinte aux droits et libertés individuelles sauf si le traitement est mis en œuvre par une autorité publique et
- Après désignation d'un DPO tenant à jour le registre de traitement et maintenant le contact avec l'Autorité.

LES OBLIGATIONS DE DILIGENCES PREALABLES

Par ailleurs, le CDN accorde une dispense de formalités (mais pas de déclaration ?) à tout traitement mis en œuvre :

- Pour un usage personnel et domestique ;
- Pour la tenue d'un registre privé ;
- Pour la tenue de comptabilité générale ;
- Pour la gestion de la paie ;
- Pour la gestion des fournisseurs et
- Par les associations loi 1901 ne concernant pas les membres et non destiné au public.

En pratique

Les déclarations les plus courantes en pratique sont faites pour les sites Internet et la vidéosurveillance.

Pour assurer la mise en conformité des sites internet, l'Autorité met à disposition sur le site www.apdp.bj un formulaire de déclaration.

OBLIGATIONS EN CAS DE TRANSFERT DE DONNEES

Un transfert, à un pays tiers, ou à une organisation internationale de données à caractères personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si les conditions définies dans le livre V sont respectées par le responsable du traitement et le sous-traitant (code du numérique, art 391).

1- TRANSFERTS FONDÉS SUR UNE DÉCISION D'ADÉQUATION

2- TRANSFERT MOYENNANT DES GARANTIES APPROPRIÉES

- Transfert décrété par le conseil des ministres après avis de l'APDP en présence de garanties appropriées
- Transfert autorisé par l'APDP en présence de garanties appropriées

OBLIGATIONS EN CAS DE TRANSFERT DE DONNEES

3- DÉROGATIONS POUR DES SITUATIONS PARTICULIÈRES

1. La personne concernée a expressément donné son consentement au transfert envisagé ;

2. Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée ;

3. Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;

4. Le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ;

5. Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;

6. Le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

OBLIGATIONS EN CAS DE TRANSFERT DE DONNEES

4- TRAITEMENT NON RÉPÉTITIF, LIMITÉ ET IMPÉRIEUX

Même si le transfert ne peut être fondé sur une décision d'adéquation ou des garanties appropriées, telles que précédemment évoquées, et même si le transfert ne bénéficie d'aucun cas de dérogation tel qu'énoncé, un transfert vers un pays tiers ou à une organisation internationale peut néanmoins avoir lieu si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personne concernée, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et liberté des personnes concernées.

Le responsable du traitement doit en outre avoir évalué toutes les circonstances entourant le transfert des données et offrir des garanties appropriées en ce qui concerne la protection des données à caractère personnel.

Le responsable de traitement doit informer l'autorité du transfert et la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.
En somme, les dérogations sont considérables et corroborées par ce cas qui paraît très spécifique mais qui concerne les transferts isolés de données susceptibles d'être particulièrement nombreux.

Merci

Pour plus de renseignements rendez-vous sur le site de l'APDP aux liens suivants :

https://www.apdp.bj
https://apdp.bj/les-outils-de-la-conformite/
https://apdp.bj/procedures/