DPDP ET MISE EN PLACE DU REGISTRE DES TRAITEMENTS

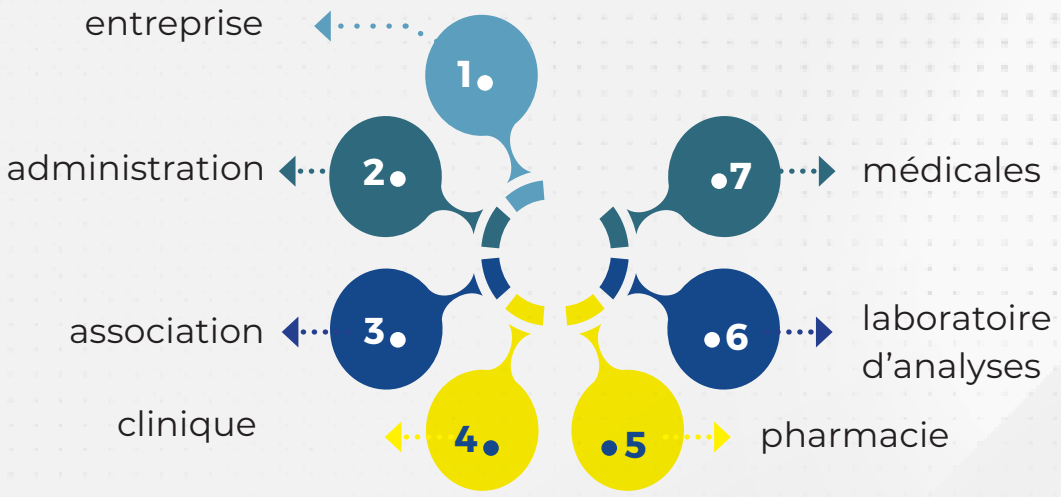
APDP, Cotonou 21 Décembre 2022

Table des matières

CARTOGRAPHIER LES TRAITEMENTS

La cartographie des traitements est une étape incontournable dans le respect des exigences de protection des données à caractère personnel.

La cartographie des traitements consiste à identifier et répertorier tous les traitements au sein d'une entité



Concrètement, elle permet à chaque responsable de traitement de déterminer, pour chaque traitement,

- le nom et les coordonnées du responsable du traitement,
- la finalité (à savoir l'objectif) dudit traitement (soins médicaux, gestion RH…),
- les catégories de personnes concernées (clients, salariés, candidats),
- les acteurs, internes ou externes, amenés à gérer ces données,
- le parcours des flux de données en cas de transferts,
- les délais prévus pour l'effacement des données
- et, enfin, une description des mesures de sécurité techniques et organisationnelles prises pour en assurer la protection.

> Bien menée, la cartographie montre avec clarté les imbrications et les interdépendances entre les multiples composants du système d'information (SI) et ses différentes couches.

A Démarche

L'idée, comme sa mise en œuvre est simple : relever le plus exhaustivement possible les traitements mis en œuvre. La cartographie des traitements de données personnelles consiste à identifier et à répertorier tous les traitements au sein de l'organisme. Concrètement, elle doit permettre d'avoir une vue d'ensemble sur :

- les différents traitements de données personnelles,
- les catégories de données personnelles traitées,
- les objectifs poursuivis par les opérations de traitement de données,
- les acteurs (internes ou externes) qui traitent ces données ;
  vous devrez notamment clairement identifier les prestataires sous-traitants,
- les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de la CEDEAO.

Pour chaque traitement de données personnelles, il faut se poser les questions ci-après :

QUI

- Inscrire dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données
- Identifier les responsables des services opérationnels traitant les données au sein de votre organisme
- Etablir la liste des sous-traitants

QUOI

- Identifier les catégories de données traitées
- Identifier les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple : les données relatives à la santé ou les infractions)

POURQUOI

- Indiquer la ou les finalités pour lesquelles vous collectez ou traitez ces données (par exemple : gestion de la relation commerciale, gestion RH…)

OÙ

- Déterminer le lieu où les données sont hébergées
- Indiquer vers quels pays les données sont éventuellement transférées

JUSQU'A QUAND

- Indiquer, pour chaque catégorie de données, combien de temps vous les conservez

COMMENT

- Préciser les mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées

Par ailleurs, deux approches souvent complémentaires, peuvent être retenues pour réaliser une cartographie et s'assurer que toutes les opérations portant sur des données personnelles ont bien été recensées : une approche métier (qui part de l'individu concerné par le traitement des données), et une approche technique (qui part du processus de gestion des données).

B Les approches

1. L'approche métier

Cette approche revient à suivre les étapes suivantes :

- **IDENTIFIER** les catégories de personnes physiques qui sont en interaction avec l'entité. Il peut ainsi s'agir des employés, des clients, des prospects, des utilisateurs, des fournisseurs, etc. ;
- **RECENSER,** pour chaque catégorie de personnes, la nature des données personnelles collectées par l'entité concernée ;
- **SUIVRE les flux de données,** à savoir leurs points d'entrée et de transfert ;
- **IDENTIFIER** les traitements effectués sur ces données.

2. L’approche technique

Cette approche repose sur la procédure suivante :

1ère étape : lister les applications contenant des données à caractère personnel

Cette première étape nécessite l’implication totale de la direction des systèmes d’information (DSI), et, notamment, des architectes et urbanistes de l’organisme. Elle consiste à établir la liste des bases de données structurées et non structurées ainsi que des applications contenant des données à caractère personnel.

L’interaction avec la DSI ne doit pas être considérée comme la base d’un inventaire des traitements de données à caractère personnel, mais principalement comme une aide pour veiller à la complétude du registre.

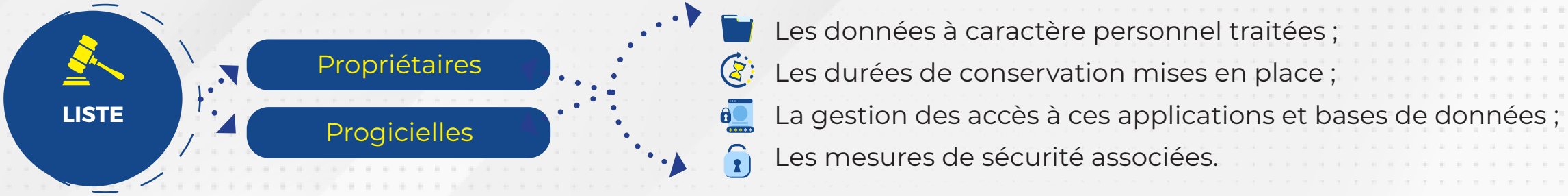
Les DSI ne raisonnent pas en finalités, mais bien en applications et en fichiers.

Attention à ne pas se perdre à ce stade dans un inventaire des données (cette étape intervient à un stade ultérieur). La phase la plus importante est bien celle réalisée auprès des directions métiers, décrite ci-après à la deuxième étape.

De plus, il convient de rappeler que le code du numérique s'impose également aux traitements de données personnelles réalisées sur supports papier et qu'il existe au sein des entreprises de plus en plus de solutions SaaS, sélectionnées à l'initiative de directions métiers et dont la DSI n'a pas connaissance.

Cette liste devra contenir deux catégories : celle des « APPLICATIONS » et bases dites « propriétaires », c'est-à-dire des applications et bases installées sur les serveurs de l'organisation et sur lesquelles celui-ci a la parfaite maîtrise, et celle des applications « progicielles », c'est-à-dire les applications tierces mises à disposition en mode **SaaS** ou sur les serveurs par des éditeurs tiers.

Pour chacune de ses données identifiées, il conviendra de lister :



Certains éditeurs proposent aujourd'hui des outils capables d'identifier des données à caractère personnel au sein de bases de données structurées et non structurées. Il faut souligner que ces outils nécessitent, d'une part, une intrusion dans les systèmes d'information de l'organisme_ ce qui peut présenter un risque, raison pour laquelle les responsables de la sécurité des systèmes d'information **(RSSI)** y sont souvent défavorables et, d'autre part, un paramétrage particulièrement coûteux.

Il est plutôt recommandé d'établir une liste des données à caractère personnel susceptibles d'être traitées par l'organisme, tant du point de vue des ressources humaines (RH) que du point de vue du cœur de son activité, et de fournir cette liste à la DSI.
Si c'est envisageable, il est également possible de faire appel à un cabinet externe spécialisé.

Il faut insister sur le fait que cette liste ne sar ait se suffire à elle-même. En effet la réglementation relative à la protection des données à caractère personnel raisonne en termes de « **finalités** » et non en termes d' **« applications »**.

La raison en est simple : une application ou une même base de données peut servir plusieurs objectifs ou finalités, chaque finalité présentant des risques différents pour les personnes concernées.
A l'inverse, la réalisation d'une même finalité peut nécessiter l'intervention de plusieurs applications. C'est la raison pour laquelle il est impératif de suivre la deuxième étape.

2e étape : identifier les processus internes impliquant un traitement des données à caractère personnel

Il s'agit ici de déterminer quelles sont les finalités pour lesquelles l'organisme traite des données à caractère personnel et sur quelles bases ces traitement s'opèrent. Pour y parvenir, un seul moyen : identifier les processus internes impliquant des traitements des données à caractère personnel.

Pour mener à bien cette étape cruciale, il est recommandé dans un premier temps de se munir d'un organigramme. Pour les organismes ne disposant pas toujours d'un organigramme complet et à jour, *il est préférable de commencer par identifier les différentes directions métiers*. Dans l'hypothèse où l'organisation de l'entité serait trop complexe, il est conseillé d'identifier un individu qui sera un relai pendant toute cette phase d'audit.

Il faudra ensuite rencontrer chaque direction métier, de préférence une personne qui connaît parfaitement les activités de sa direction et qui en aurait une vue d'ensemble.

Il faut garder à l'esprit que ces entretiens avec les directions métiers ont pour objectif de déterminer les processus internes impliquant des données personnelles, et qui faudra donc en sortir avec non seulement une liste de ces processus, mais également une liste de finalités précises pour lesquelles les données sont traitées.

D'une manière générale, il est recommandé de conduire ses entretiens selon la trame suivante :

- rappel du contexte, des enjeux et des définitions essentielles (qu'est-ce qu'une donnée à caractère personnel, un traitement, etc.) ;
- liste des activités de la direction ou du département ;
- identification des processus internes impliquant des données personnelles ;
- identification des finalités pour lesquelles les données sont traitées
- identification des conditions de traitement de ces données, et notamment :

- **quelles sont les données collectées ?**
- **comment ces données sont-elles collectées ?**
- **sont-elles transmises ou accessibles à des tiers ? Si oui, par quelle entité ou département ? Sur la base de quel contrat ?**
- **sont-elles transmises ou accessibles depuis un pays situé en dehors de la CEDEAO ?**

Sur la base de ses éléments, il est enfin possible d'établir un premier inventaire des traitements sous forme d'un registre des activités de traitement.

A ce stade, il faut éviter deux erreurs courantes :

1. la première est de ne pas s'en tenir à un inventaire, mais essayer de réaliser simultanément un audit, une sensibilisation des personnels et une formalisation des actions de mise en conformité. Il vaut mieux privilégier une approche progressive et revenir plusieurs fois sur le sujet. L'objectif prioritaire est de disposer d'un inventaire dans les grandes lignes. Le DPO peut ensuite revenir vers certains interlocuteurs afin d'affiner son registre, en priorité sur les finalités les plus sensibles.

2. la seconde erreur consiste à vouloir réaliser cet inventaire en diffusant un questionnaire destiné à être renseigné par les directions métiers. Cela suppose que les concepts de base du code du numérique soient maîtrisés par les personnes sollicitées, ce qui est rarement le cas.

CLASSIFIER LES DONNEES

L'article 1 du Code du numérique dispose en effet qu'il faut entendre par 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...***

Pour autant, il n’est pas subversif de relever que les données à caractère personnel objet des droits garantis aux personnes prennent en compte les onze (11) autres types de données que le Code du numérique a pris le soin de définir expressément. Ainsi, les droits reconnus aux personnes par le Code du numérique sur leurs données à caractère personnel, portent sur :

- Les données afférentes à la création de signature
- Les données biométriques
- Les données concernant la santé
- Les données de création de cachet électronique
- Les données d’identification personnelle
- Les données génétiques
- Les données informatiques
- Les données relatives aux abonnés
- Les données relatives au contenu
- Les données relatives au trafic
- Les données sensibles

La démarcation la plus importante à opérer ici est donc bien celle entre les données sensibles et les autres données.

En effet, tandis que les autres sont quasiment libres de traitements, le traitement des données sensibles est interdit. Sauf, à se retrouver dans les cas limitatifs indiqués par la loi.

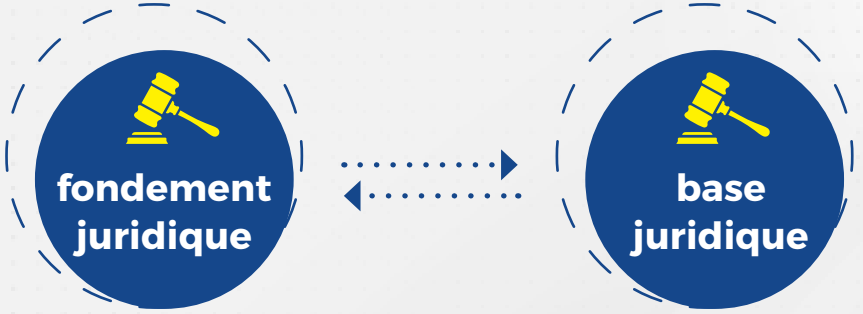
A l'issue de l'exercice, il faudra déterminer les bases légales des traitements effectués avec les données détenues afin de réussir l'étape suivante du remplissage de son registre des activités de traitement.

III

DETERMINER LES BASES LEGALES DE TRAITEMENT DES DONNEES

Pour pouvoir être mis en œuvre, tout traitement de données doit se fonder sur l'une des **« bases légales »** prévues par le Code du numérique. La détermination de la base légale appropriée est une étape-clé pour les organismes.

La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement.



Il est permis de traiter des données personnelles lorsque le traitement repose sur une des 6 bases légales mentionnées au Code du numérique :

1. **le consentement :** la personne a consenti au traitement de ses données ;
2. **le contrat :** le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;
3. **l'obligation légale :** le traitement est imposé par des textes légaux ;
4. **la mission d'intérêt public :** le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
5. **l'intérêt légitime :** le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées ;
6. **la sauvegarde des intérêts vitaux :** le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers.

Lorsqu'un même traitement de données poursuit plusieurs finalités, c'est-à-dire plusieurs objectifs, une base légale doit être définie pour chacune de ces finalités.

En revanche, il n'est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule.

Exemple : un fichier « clients et prospects » d'une entreprise peut poursuivre plusieurs finalités, qui doivent chacune reposer sur une base légale : le contrat pour la gestion des commandes, des livraisons ou du service après-vente ; l'obligation légale pour la tenue de la comptabilité ; le consentement pour les opérations de prospection commerciale par messagerie ; etc.

Il est extrêmement rare qu'une direction métier ait les compétences pour déterminer le fondement du traitement. Or, ce choix est essentiel, car il a un impact, par exemple, sur le droit d'opposition des personnes concernées.
L'expertise du DPO est crucial.

Dans le cas où l'intérêt légitime du responsable du traitement serait retenu les droits des personnes concernées peuvent être légitimés. Si le traitement est basé sur le consentement, le DPO veillera à la validité de celui-ci, qui doit pouvoir être prouvé par le responsable du traitement.

Tel que défini par le Code du Numérique, le registre ne permet pas à un DPO d'être efficient. Il lui appartient d'enrichir ce document des informations qui lui paraissent indispensables à sa pratique professionnelle (indicateur de sensibilité du traitement, date de la dernière revue ou du dernier audit, existence d'une analyse d'impact, date et nature de la dernière violation de données ayant affecté ce traitement, outil informatique principal utilisé, etc.)

A Critère transversal : la nécessité

> Traitement nécessaire…

Notion Autonome en droit européen : décision Huber de la CJCE, C524/06 Heinz Huber v Bundesrepublik Deutschland 18 décembre 2008
Pas de moyen moins intrusif pour atteindre la finalité poursuivie
≠ utile
≠ simple moyen pour atteindre l'objectif : obligation de sécurité qui pèse sur l'employeur ne peut fonder un système de vidéosurveillance (autre base légale = intérêt légitime)

B Le consentement comme fondement d'un traitement de données

Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement. Le consentement est donc l'un des fondements possibles d'un traitement de données.

Le consentement est défini à l'article 1 du Code du Numérique comme

> toute manifestation de **volonté expresse, non équivoque, libre, spécifique et informée** par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte par une déclaration ou par un acte positif clair que les données à caractère personnel le concernant fassent l'objet d'un traitement

1. Conditions applicables au consentement

Eclairé : volonté expresse et informée

- La personne concernée doit être informée au moment de la collecte.
- La demande de consentement doit être présentée “sous une forme compréhensible et aisément accessible et formulée dans des termes clairs et simples “.
- Exemple: http://mashable.france24.com/mashallow/20170713 nettoyer toilette conditions générales wifi

Spécifique

- La personne concernée a consenti au traitement de ses données pour “une ou plusieurs finalités spécifiques”.
- ≠Générales
- Le consentement est présumé ne pas avoir été donné librement “si un consentement distinct ne peut pas être donné à différentes opérations de traitement [...] bien que cela soit approprié dans le cas d’espèce” d’espèce”(considérant 43)

Libre

- « Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d’une véritable liberté de choix ou n’est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice », considérant 42.
- Cas particulier : existence d’un déséquilibre manifeste entre la personne concernée et le responsable du traitement

Univoque

- Le consentement doit être donné par un acte positif clair par lequel la personne concernée manifeste [...] son accord au traitement des données qui la concerne, par exemple au moyen d’une déclaration écrite ou orale, en cochant une case, etc.
- Pas de consentement tacite

2. La preuve du consentement

Traçabilité : « le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant », art. 390 al 1

« Le responsable de traitement doit être en mesure de prouver que ladite personne a consenti à l'opération de traitement », considérant 42 : process générique de recueil du consentement est donc insuffisant.

3. Le retrait du consentement

- La personne a le droit de retirer son consentement à tout moment.
- Le retrait ne compromet pas la licéité du traitement effectué avant ce retrait
- La personne en est informée avant de le donner.
- Il est aussi simple de retirer que de donner son consentement

4. Le consentement et la collecte de données particulières

Article 394

- Bases légales spécifiques listée à l'article 394
- Interdiction de collecter des données particulières sauf si « la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit en vigueur en République du Bénin prévoit que l'interdiction visée à l'alinéa 1 ne peut pas être levée par la personne concernée.»

5. Le consentement et la collecte de données d'un enfant mineur

En ce qui concerne l'offre directe de services de la société de l'information aux mineurs, le traitement des données à caractère personnel relatives à un mineur est licite lorsque le mineur est âgé d'au moins seize (16) ans.

Pour les moins de seize (16) ans, le traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard du mineur.

Il faut vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

Pas applicable à tous les traitements concernant des mineurs
Définition de l'offre de services de la société de l'information directive 2015/1535 : « tout service de la société de l'information, c'est à dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services »

6. Le consentement et les transferts de données vers un Etat tiers

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 lorsque la personne concernée a expressément donné son consentement au transfert envisagé ;», article 392

Article 392

C Contrat auquel la personne est partie ou l'exécution de mesures précontractuelles

- Le responsable du traitement doit être en mesure de démontrer :
- L'existence d'un contrat « valide » et
- Que le traitement est nécessaire à l'exécution du contrat (objectivement) évaluation de la nécessité.

Quelle est la nature du service fourni ? Quelles en sont les caractéristiques ?
Quels sont les éléments importants du contrat ?
Quelles sont les attentes des parties au contrat ?
Comment le service a-t-il été promu, publié ou vendu à la personne concernée ?
Un consommateur moyen accepterait-il pour les mêmes bénéfices ?

- Référence aux attentes raisonnables de la personne concernée
- Si le contrat consiste en plusieurs services, l'évaluation doit être réalisée service/service
  Contrat entre le responsable du traitement et la personne concernée et non nécessaire à l'exécution d'un contrat entre un responsable du traitement et un tiers : exigence d'un lien contractuel direct
- Ou de mesures précontractuelles prises à la demande de la personne concernée et non à l'initiative du RT (en aucun cas, les publicités non sollicitées à l'initiative du responsable de traitement ou d'un tiers ne peuvent être considérées comme des mesures précontractuelles ou nécessaires à l'exécution du contrat)

D Respect d'une obligation légale

1. Définition et conditions de l'obligation légale

- L'obligation légale doit être définie par le droit positif national ou celui d'un Etat membre auquel le RT est soumis (loi, décret, etc.)
- Obligation impérative de traiter des données personnelles suffisamment claire et précise : le RT ne doit pas avoir le choix de se conformer ou non à l'obligation. Une possibilité ou une autorisation ≠ d'une obligation légale.

  ≫ Exemple : l'obligation générale d'assurer la sécurité des données n'est pas assez précise pour constituer une obligation légale de mise en œuvre d'un traitement de lutte contre les intrusions.

- La disposition en question doit définir les finalités du traitement (exemple de certains dispositifs d'alerte dans le cadre de la loi anti-blanchiment)
- Cette obligation doit s'imposer au responsable du traitement et non aux personnes concernées (obligation de déclaration des impôts à l'administration fiscale s'impose aux contribuables et donc, ne peut pas servir de fondement aux traitements mis en œuvre par l'administration.)

2. Conséquences pour les personnes concernées

Les droits suivants ne sont pas applicables :

- Le droit d'opposition,
- Le droit d'effacement et
- Le droit à la portabilité.

E Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique

1. Définition de l'intérêt vital

- Aux termes du Considérant 46 du groupe de travail G29 : « intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique »
- « Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine »

7. Conditions

- Généralement situation exigeant le traitement de données médicales d'ailleurs également l'une des bases légales permettant de traiter des données de santé
- Base légale qui ne peut pas servir à justifier l'ensemble des traitements de données de santé uniquement des situations d'urgence
- Intérêt vital de la personne concernée ou d'un tiers (par exemple un enfant)

F Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement

1. Qui peut utiliser cette base légale ?

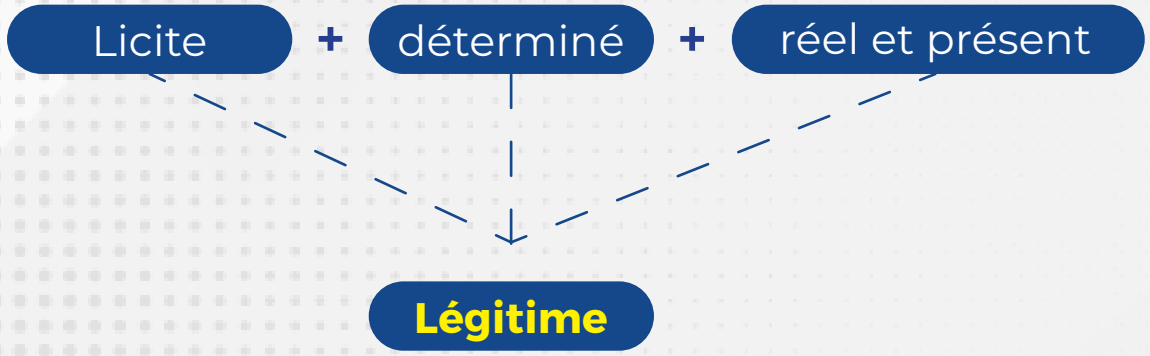
- Les autorités publiques or organismes chargés d'une mission de services publiques
- La mission d'intérêt publique doit être définie dans les dispositions légales (droit communautaire ou droit national)
- Ces dispositions peuvent définir les finalités du traitement et les conditions essentielles de sa mise en œuvre (pas obligatoire).
- Exemples de l'APDP : Gestion des demandes du public, des plaintes, des demandes de droit d'accès indirect, etc.

8. Conséquences pour les personnes concernées

- Le droit à la portabilité n'est pas applicable.
- Le droit à l'effacement reste conditionné.
- Pas de droit au retrait du consentement.

G Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers

- Traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant
- Exemples : prévention de la fraude, traitement à des fins de prospection, etc.

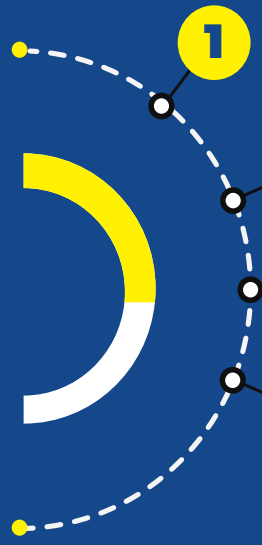


L’intérêt légitime du responsable de traitement doit être mis en balance avec les droits fondamentaux et la liberté des personnes concernées ; les responsables de traitements peuvent avoir un intérêt légitime dans la connaissance des préférences de leurs clients pour leur permettre de personnaliser leurs offres et au final offrir des produits et services qui correspondent aux besoins et désirs des clients. Ainsi, l’intérêt légitime peut être un fondement légal approprié pour être utilisé pour certains types d’activité marketing on line et offline, à condition que des mesures appropriées soient prévues (notamment, un mécanisme fonctionnel permettant d’objecter à un tel processus).

9. La balance des intérêts

- Nature des données traitées (sensibilité des données)
- Modalités de traitement (étude d'un comportement, d'une personnalité
- Incidences négatives sur les droits de la personne (exclusion, décision, répercussion morale)
- Incidences positives (amélioration de la qualité du service)
- Nombre de personnes concernées
- Attentes raisonnables de la personne concernée (statut du responsable de traitement, nature du service fourni, obligations légales ou contractuelles)

10. Méthode



Etape 1 : Qualification de l'intérêt légitime du responsable du traitement ou du tiers

Etape 2 : Analyse du caractère nécessaire du traitement pour la réalisation de l'intérêt poursuivi

Etape 3 : Bilan provisoire permettant d'apprécier si les droits fondamentaux ou les intérêts des personnes concernées prévalent sur l'intérêt poursuivi par le responsable du traitement

Etape 4 : Mise en place de garanties supplémentaires (anonymisation, transparence accrue...)

11. Garanties

Les garanties et les mesures adéquates peuvent dans le cas d'une ingérence même grave dans la vie privée dans le cadre d'un intérêt impérieux poursuivi par le responsable de traitement réduire les incidences du traitement et ainsi modifier l'équilibre des droits et intérêts au point où celui du responsable prévaut.

H Intérêt légitime et organismes publics

- Exclusion traitements effectués par des autorités publiques dans l'accomplissement de leurs missions (utiliser l'intérêt public)
- Ne signifie pas qu'une autorité publique ne peut pas utiliser l'intérêt légitime comme base légale mais pas pour l'exercice de ses missions

IV

TENIR À JOUR SON REGISTRE DES ACTIVITÉS DE TRAITEMENT

A Le contenu

Les informations qui doivent figurer dans le registre des activités de traitement sont limitativement énumérées à **l'article 435 du CDN**, à savoir :

- Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable de traitement et du DPO ;
- Les finalités du traitement ;
- Une description des catégories de personnes concernées et des catégories des données à caractère personnel ;
- Les catégories de destinataires auxquels les données de caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 491 al 2 du CDN, les documents attestant de l'existence de garanties appropriées ;

- Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniquement organisationnelles de sécurité du traitement visées à l'article 435 al 1 du CDN.

A titre liminaire, il est important de noter que les durées de conservations et les mesures techniques et organisationnelles de sécurité du traitement doivent figurer dans le registre sous la mention **« dans la mesure du possible ».**

En pratique, cela signifie que si pour obtenir ses informations, des efforts disproportionnés doivent être réalisés par l'organisme, l'Autorité accepterait qu'elles n'y figurent pas.

Le registre étant la pierre angulaire du DPO, celui-ci a tout intérêt à ce que ce document soit le plus complet possible et qu'il soit le reflet fidèle de la réalité.

Concernant, par exemple, les durées de conservation, cette information est exigée par les agents de l'APDP lors d'une mission de contrôle sur place.

La détermination des durées de conservation n'est pas le fait du DPO ni de la DSI, mais bien de la direction métiers.

Le DPO peut, par contre, apporter son expertise pour faire en sorte que celle-ci soit proportionnée à la finalité visée.

Il est prudent également chercher à définir, en sus de la durée de conservation en archives courantes (pour la finalité), la durée de conservation en archives intermédiaires (par exemple en cas de litige).

B Mettre à jour le registre des activités de traitement

1. Importance de la mise à jour du registre

Démontrer sa conformité vis-à-vis de l'APDP

Il appartient au responsable du traitement ou au sous-traitant (et, le cas échéant, à leur représentant) de mettre le registre à la disposition de l'Autorité sur demande de celle-ci.

Il est donc essentiel, non seulement, que ce registre soit établi, mais également qu'il soit mis à jour. La tenue à jour du registre (comme son établissement) permet à l'Autorité de bénéficier d'une vue générale de l'ensemble des traitements mis en œuvre et à jour.

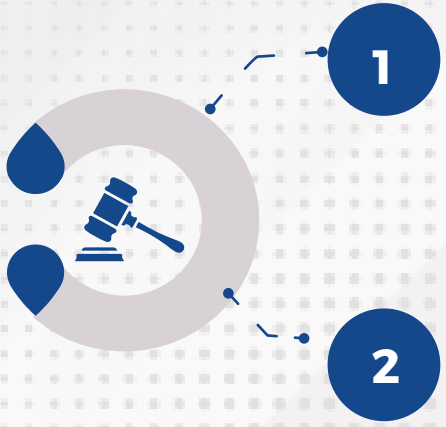
Le maintien à jour du registre est surtout un moyen pour le responsable du traitement et le DPO de connaître en permanence l'état de l'inventaire des traitements, et de pouvoir en assurer la supervision.

Éviter les sanctions

La mise à jour (comme l'établissement du registre) permettra d'éviter les sanctions prévues par le Code du Numérique, faute de pouvoir démontrer la conformité face à un contrôle de l'APDP. Cette mise à jour constitue à la fois un prérequis et l'un des moyens de démontrer sa conformité.

12. Le DPO, acteur indispensable de la tenue du registre

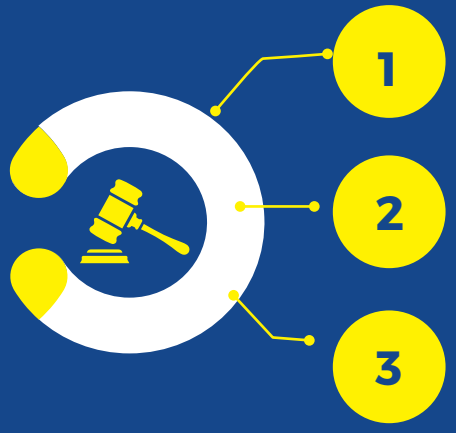
Les différents services de l'organisme notifient au DPO :



1. tout changement dans le traitement des données ;
2. toute échéance afin que le registre soit mis à jour ;

Dans le cadre d'un groupe de sociétés, des relais peuvent être mis en place au sein de chaque entité afin de faire remonter les notifications au DPO, s'il n'y en a qu'un seul pour le groupe. Pour effectuer cette notification, une classification peut être mise en place selon le degré de criticité des traitements considérés. A titre d'exemple, il peut exister des notifications prioritaires pour les traitements de données sensibles, les traitements à risque, etc.

Il est recommandé que le DPO soit le pilote de la tenue du registre. Dans ce cadre, il revient au DPO :



1. de déterminer la structure, l'outil de gestion, les modalités d'utilisation du registre ainsi que les modalités d'accès ;
2. de créer les fiches du registre, aidé de ses éventuels relais et ;
3. de valider la complétude.

1. Lorganisme

1. Informations sur l'organisme				
Dénomination	N° IFU	RCCM	Tél	Email

2. Coordonnées du Responsable de la Structure (Responsable de Traitement ou son Représentant)				
Nom et Prénoms	Fonction	Adresse	Tél	Email

3. Nom et coordonnées du Délégué à la Protection des Données					
Nom et Prénoms	**Fonction**	**Statut**	**Adresse**	**Tél**	**Email**

13. Activités de l'organisme impliquant le traitement de données personnelles

Ici, il convient de lister ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (à adapter le cas échéant)
Activités 1	Gestion de la paie
Activités 2	Gestion des clients/prospects
Activités 3	Gestion des fournisseurs
Activités 4	Gestion des ressources humaines
Activités 5	Géolocalisation
Activités 6	Vidéosurveillance
Activités 7	Gestion des contraventions
Activités 8	Comptabilité générale

14. Fiche de registre : Clients/prospects

(Reprise de l'activité 2 de la liste des activités)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du logiciel ou de l'application (si pertinent)	

Objectifs poursuivis

Décrivez ici clairement l'objet du traitement de données personnelles et ses fonctionnalités.

- Opérations relatives à la gestion des clients concernant : les contrats ; les commandes ; les livraisons ; les factures ; la comptabilité et en particulier la gestion des comptes clients ; *(le cas échéant)* le suivi de la relation client tel que la réalisation d'enquêtes de satisfaction, la gestion des réclamations et du service après-vente ;
- Opérations relatives à la prospection (sollicitations, promotions, sondages, tests produits, actions de fidélisation, etc.) ;
- Élaboration de statistiques commerciales ;
- *(le cas échéant)* Organisation de jeux concours, de loteries ou de toute opération promotionnelle (à l'exclusion des jeux d'argent et de hasard en ligne soumis à l'agrément de la Loterie Nationale du Bénin (LNB) ;
- Gestion des demandes d'exercice des droits légaux prévus par le Code du Numérique ;
- *(le cas échéant)* Gestion des avis des personnes sur des produits, services ou contenus.

Catégories de personnes concernées

Listez ici les différents types de personnes dont vous collectez ou utilisez les données.

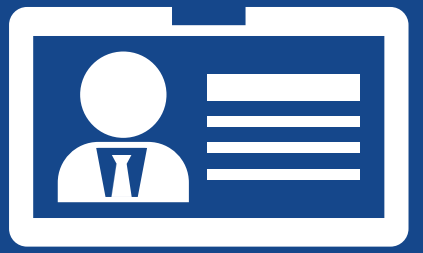
1. Clients ;
2. Prospects ;
3. (le cas échéant) Utilisateurs de services de communication en ligne.
4. Etc.

Catégories de données collectées

Listez ici les différentes données traitées (à adapter le cas échéant)

Etat-civil, identité, données d'identification, images

Civilité, nom, prénoms, adresse, numéro de téléphone (fixe et/ou mobile), numéro de télécopie, adresses de courrier électronique, date de naissance, code interne de traitement permettant l'identification du client. Une copie d'un titre d'identité peut être conservée aux fins de preuve de l'exercice des droits légaux prévus par le Code du Numérique ou pour répondre à une obligation légale.



Vie personnelle

Vie maritale, nombre de personnes composant le foyer, nombre et âge du ou des enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle.

Informations d'ordre économique et financier

Relevé d'identité postale ou bancaire, numéro de chèque, numéro de carte bancaire, date de fin de validité de la carte bancaire, cryptogramme visuel, modalités de règlement, remises consenties, reçus, soldes et impayés et informations relatives aux crédits souscrits (montant et durée, nom de l'organisme prêteur) en cas de financement de la commande par crédit, numéro de la transaction, détail de l'achat, de l'abonnement, du bien ou du service souscrit.

Autres catégories de données :

Suivi de la relation commerciale : Demandes de documentation, demandes d'essai, produit acheté, service ou abonnement souscrit, quantité, montant, périodicité, adresse de livraison, historique des achats et des prestations de services, retour des produits, origine de la vente (vendeur, représentant, partenaire, affilié) ou de la commande, correspondances avec le client et service après-vente, échanges et commentaires des clients et prospects, personne(s) en charge de la relation client.

***(le cas échéant)* Organisation et au traitement des jeux concours, de loteries et de toute opération promotionnelle :**

- Date de participation,
- réponses apportées aux jeux concours et nature des lots offerts.

***(le cas échéant)* Utilisation d'un service de communication en ligne (site internet) :** Données du profil utilisateur (ex : pseudonyme), données de connexion (date, heure, adresse internet, caractéristiques techniques du terminal de l'utilisateur, pages consultées) et avis/contenu postés en ligne

Des données sensibles sont-elles traitées ?

Oui ☐ ***Non*** ☐

Si oui, lesquelles ?

Durées de conservation des catégories de données

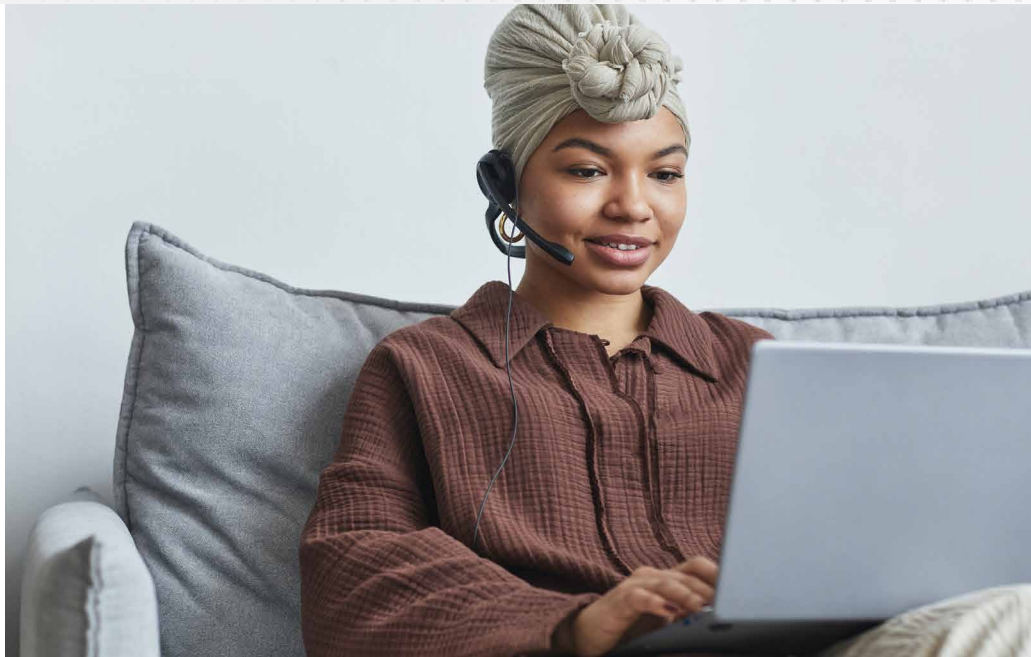
Combien de temps conservez-vous ces informations ?

jours, mois, ans ☐ ***Autre durée :*** ☐

Etat-civil, identité, données d'identification, images /Vie personnelle/Informations d'ordre économique et financier/Suivi de la relation commerciale/*(le cas échéant)* Organisation et au traitement des jeux concours, de loteries et de toute opération promotionnelle : Fin de la relation commerciale, sauf autorisation du client ou durée spécifique imposée par une disposition légale ou réglementaire.

Les données utilisées à des fins de prospection commerciale sont conservées pendant trois ans à compter de la fin de la relation commerciale (ou de la collecte pour les prospects non clients).

***(le cas échéant)* Utilisation d'un service de communication en ligne (site internet) :** Suppression du compte par l'utilisateur ou après [insérer durée raisonnable pour l'entreprise] d'inutilisation du compte. Les données collectées via des Cookies sont supprimées après 13 mois.



Catégories de destinataires des données

Destinataires internes

1. Personnes habilitées à traiter les données au sein de l'entreprise.

2. _

Organismes externes

1. Pouvoirs publics

2. _

Sous-traitants (à compléter par l'entreprise)

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. _

2. _

3. _

4. _

Transferts des données hors CEDEAO (à vérifier par l'entreprise

Des données personnelles sont-elles transmises hors de l'Union européenne ?

Oui ☐ ***Non*** ☐

Si oui, vers quel(s) pays?

Dans des situations particulières (transfert vers un pays tiers non couvert, et sans les garanties mentionnées aux articles 391 et 392 du Code du Numérique), des garanties spécifiques devront être prévues et documentées dans le registre (article 435 du Code du Numérique).

Mesures de sécurité (à compléter par l'entreprise)

Décrivez ici les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Contrôle d'accès des utilisateurs

Décrivez les mesures :

Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs), les données enregistrées (exemple : identifiant, date et heure de connexion, etc.)* **et leur durée de conservation :**

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les modalités :

Chiffrement des données

Décrivez les mesures (exemple : site accessible en https, utilisation de TLS, etc.) :

Contrôle des sous-traitants

Décrivez les modalités :

Autres mesures :

MERCI