



LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

Par Ambroise Dj. ZINSOU
Consultant formateur indépendant
Management Télécoms & TIC et Protection
des données personnelles et de la vie privée



SOMMAIRE

- I. INTRODUCTION
- II. NOTIONS DE RESPONSABLE DE TRAITEMENT ET DE SOUS- TRAITANT ET RESPONSABLE CONJOINT
- III. L'OBLIGATION POUR LE RESPONSABLE DU TRAITEMENT D'ÊTRE « ACCOUNTABLE »
- IV. LE PRINCIPE DE « PRIVACY BY DESIGN »
- V. LE PRINCIPE DE « PRIVACY BY DEFAULT »
- VI. LES FORMALITÉS OBLIGATOIRES EN CAS DE RESPONSABILITÉ CONJOINTE
- VII. ROLE DU SOUS -TRAITANT



I. INTRODUCTION

La loi N° 2017-20 du 20 Avril 2018 portant Code du numérique en République du Bénin instaure un cadre juridique qui renforce les responsabilités des responsables de traitement, des sous-traitant et des responsables conjoints. En effet, le code modifie substantiellement la façon d'appréhender la conformité à la réglementation relative à la protection des données. Un nouveau principe clé voit donc le jour, le principe d'« ACCOUNTABILITY » qui consiste à laisser plus de marge de manœuvre aux responsables de traitement et à leur(s) sous-traitant(s) pour assurer la conformité de leurs traitements au cadre légal en vigueur tout en leur exigeant d'être en mesure de pouvoir démontrer, prouver, la conformité des traitement à la loi.

De ce principe clé, découlent également d'autres nouveaux principes : le principe de « privacy by design » et le principe de « privacy by default » [Art. 424 du CDN] qu'il reviendra aux différents responsables de traitement d'intégrer dans leur politique de mise en conformité

Le responsable du traitement devient donc l'acteur majeur de cette conformité et il se doit de s'assurer que les traitements de données qu'il effectue respectent bien la loi.



II. NOTIONS DE RESPONSABLE DE TRAITEMENT ET DE SOUS- TRAITANT ET RESPONSABLE CONJOINT

2.1. Définitions

2.1.1. Notion sur le responsable de traitement

Le Responsable du traitement est défini 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

Cette définition se compose principalement de trois éléments qu'il revient d'analyser distinctement :

- 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.



II. NOTIONS DE RESPONSABLE DE TRAITEMENT ET DE SOUS- TRAITANT ET RESPONSABLE CONJOINT

i. La personne physique ou morale, l'autorité publique, le service ou un autre organisme

indique qu'une personne physique ou une personne morale peut devenir responsables du traitement. Cependant en terme de responsabilité, si une personne physique traite des données à caractère personnel dans le cadre de ses missions au sein d'une personne morale, la personne physique n'est pas considérée comme responsable de ce traitement. La personne morale demeurera seule responsable de celui-ci que la personne physique ne met pas en œuvre des opérations de traitement pour son compte propre.

Le fait qu'une entreprise désigne explicitement une personne comme responsable de la gestion des données n'aura pas pour conséquence de déplacer la responsabilité du traitement sur celle-ci. L'entreprise restera donc seule responsable

De même, dans l'hypothèse où un employé d'une personne morale vient à utiliser des données à caractère personnel dans le cadre de ses activités professionnelles, mais sans l'autorisation de sa hiérarchie, la personne morale demeure malgré tout responsable du traitement.



II. NOTIONS DE RESPONSABLE DE TRAITEMENT ET DE SOUS- TRAITANT ET RESPONSABLE CONJOINT

Cependant, si une personne physique utilise les données d'une entreprise ou d'un organisme public à des fins privées, cette personne devra alors être considérée comme unique responsable pour Les nouveaux traitements

ii. Qui détermine les moyens et les finalités

L'expression « **détermine les finalités et les moyens** » fait référence au pouvoir de décision, à l'autonomie, que doit avoir une partie pour être qualifiée de responsable du traitement.

Identifier qui est responsable du traitement? revient à identifier qui prend les décisions importantes concernant le traitement et qui est investi de l'autorité pour déterminer les caractéristiques principales d'un traitement : son objectif, ses méthodes, les moyens et les finalités.

Toute personne qui détermine la finalité de ce traitement est de facto responsable du traitement puisqu'elle a un pouvoir de décision sur un élément essentiel du traitement. À l'inverse, un sous-traitant ne peut pas lui-même déterminer une finalité sans sortir de son rôle de simple exécutant.



II. NOTIONS DE RESPONSABLE DE TRAITEMENT ET DE SOUS- TRAITANT ET RESPONSABLE CONJOINT

iii. Seul ou conjointement

Dans les cas où les finalités et les moyens du traitement sont déterminés par plusieurs entités juridiques distinctes, toutes celles-ci seront responsables conjoints du traitement qu'elles mettent en œuvre.

La responsabilité conjointe ne se limite pas au cas où « les entités déterminent conjointement et partagent l'ensemble des finalités et des moyens des opérations de traitement. Il existe en effet d'autres formes de responsabilité conjointe. Il arrive régulièrement que plusieurs entreprises partagent les mêmes moyens pour des finalités propres. Elles seront dans ce cas responsables conjoints des moyens utilisés pour récolter ces données mais resteront chacune seule responsable du traitement subséquent de ces données. [**Art. 388 du CDN**]

Dans ce cas, ils sont liés par un accord cadre reflétant les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées.



II. NOTIONS DE RESPONSABLE DE TRAITEMENT ET DE SOUS- TRAITANT ET RESPONSABLE CONJOINT

- **2.1.2. La notion de « sous-traitant »**

Au sens du Code, un sous-traitant est toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement [page 49 du CDN] dont les responsabilités sont précisées à l'article 386 du CDN;

Ce « sous-traitant » est soit une organisation extérieure à celle du responsable du traitement , et dispose donc d'une existence propre. Il est indépendante du responsable du traitement et n'est pas entièrement intégré au fonctionnement interne du responsable du traitement.

Le sous-traitant se contente d'exécuter les instructions données par le responsable du traitement, au moins en ce qui concerne la finalité du traitement et les éléments essentiels des moyens.



III. L'OBLIGATION POUR LE RESPONSABLE DU TRAITEMENT D'ÊTRE « ACCOUNTABLE »

3.1. Principe d'« ACCOUNTABILITY » en matière de protection des données

Le Code a introduit un nouveau principe en matière de protection des données personnelles, celui d'« **ACCOUNTABILITY** ». Autrement dit, le responsable du traitement doit être « en mesure de rendre des comptes ».

Ce nouveau principe d'« **ACCOUNTABILITY** » vise à davantage responsabiliser les responsables de traitement en leur laissant plus de marge de manœuvre dans les choix qu'ils font afin d'assurer la conformité de leur traitement au livre Vème du Code.

Le responsable du traitement a donc plus de liberté qu'auparavant concernant les mesures à mettre en place pour assurer le respect du cadre légal, mais il est également responsable de ses choix et doit pouvoir démontrer qu'il a bien fait le nécessaire pour être conforme à la loi.

Toutefois, le responsable du traitement est certes plus responsabilisé, mais le Code ne le laisse pas complètement libre sur la manière de se conformer au règlement et impose certaines mesures qui sont particulièrement importantes et nécessaires :



III. L'OBLIGATION POUR LE RESPONSABLE DU TRAITEMENT D'ÊTRE « ACCOUNTABLE »

- l'obligation pour le responsable de tenir un registre [art. 435 du CDN] ;
- d'effectuer des analyses d'impact [art. 428 du CDN] ;
- de désigner un DPO [art. 430 du CDN] ;
- de respecter les principes de « privacy by design » et « privacy by default » [art. 434 du CDN] ;
- de recourir à des BCR [Binding Corporate Rules –Règle d'entreprise contraignante] [Art. 391 du CDN]

3.2. L'« ACCOUNTABILITY » en tant qu'obligation générale pour le responsable du traitement

Les articles 424, 426, 427 énoncent les deux éléments de base du principe d'« accountability » puisqu'il prévoit que « [...] le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément aux dispositions du livre Vème du Code [Art. 387 point 1 à 14 du CDN]



III. L'OBLIGATION POUR LE RESPONSABLE DU TRAITEMENT D'ÊTRE « ACCOUNTABLE »

Le responsable du traitement devra notamment prendre en compte :

- le type et le contexte du traitement ;
- la nature des données (données sensibles ou non) ;,
- les finalités poursuivies, et ;
- les risques que font peser ce traitement sur la vie privée des personnes concernées.

Ainsi, sur la base de ces éléments, le responsable de traitement sera à même de mettre en œuvre des mesures protectrices et organisationnelles adaptées à la situation.

L'évaluation des risques et des mesures censées les empêcher ou les diminuer à un niveau acceptable se confondra parfois avec l'analyse d'impact prévue à l'article 428 Code. Si cette disposition n'impose pas systématiquement cette analyse pour tous les traitements, une analyse minimale est dans tous les cas nécessaire pour apprécier l'adéquation des mesures mises en œuvre avec les risques encourus pour les personnes concernées



III. L'OBLIGATION POUR LE RESPONSABLE DU TRAITEMENT D'ÊTRE « ACCOUNTABLE »

Sur la notion d'« **ACCOUNTABILITY** », nous citerons, à titre d'exemples de mesures organisationnelles applicables :

- la formation de son personnel aux grands principes de la protection des données ;
- la mise en place de procédures de gestion des demandes découlant des droits conférés aux personnes concernées ;
- les procédures de notification en cas de violation de données et la mise en place d'audits internes ou externes permettant de tester le fonctionnement de ces différentes procédures.

Pour les mesures relatives à la sécurité des données, l'article 426 du CDN énumère quelques techniques comme le chiffrement et la pseudonymisation des données



III. L'OBLIGATION POUR LE RESPONSABLE DU TRAITEMENT D'ÊTRE « ACCOUNTABLE »

3.3. Pouvoir démontrer la conformité des traitements [Art. 387.4 du CDN]

Le responsable du traitement doit non seulement mettre en place les mesures nécessaires afin d'assurer le respect du Code, mais il doit également pouvoir le démontrer.

Concrètement, cela signifie que le responsable du traitement a l'obligation de documenter les traitements qu'il effectue, d'expliquer les choix qu'il pose et de garder les preuves des mesures techniques et organisationnelles qu'il a prises.

En cas de contrôle par une autorité de protection des données, le responsable du traitement sera amené à démontrer qu'il réalise des traitements de données personnelles de manière conforme à la loi. Il devra donc, par exemple, justifier (documents à l'appui) pourquoi il a considéré qu'il ne devait pas désigner par exemple un DPO. Pour ce faire, il pourrait notamment donner à l'autorité de protection des données une note détaillée, dans laquelle il précise les raisons de son choix de ne pas désigner de DPO.



PRINCIPE DE « PRIVACY BY DESIGN - LA PROTECTION DES DONNÉES PERSONNELLES DES LA CONCEPTION »

3.3. Pouvoir démontrer la conformité des traitements [Art. 387.4 du CDN]

L'approche Privacy By Design consiste à adopter dès la conception et par défaut, des mesures organisationnelles et techniques appropriées pour garantir la protection de la vie privée des personnes concernées par le traitement et non à la fin du processus, et ainsi de mettre en place, à temps, des mesures techniques et organisationnelles appropriées pour garantir le respect des exigences de la loi. En d'autres termes, le responsable du traitement doit adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception du traitement

Il s'agit de favoriser l'économie numérique tout en créant un environnement de confiance.

En effet avec le Code, la donnée pour être source de richesse , doit être conforme aux attentes des utilisateurs. Cette confiance passe par un renforcement de la protection et de la sécurité des données des utilisateurs.



V. LE PRINCIPE DE « PRIVACY BY DEFAULT - LA PROTECTION DES DONNÉES PERSONNELLES PAR DÉFAUT »

5.1. Le privacy by default

Le privacy by default est l'idée qu'une fois que l'on a mis en place un système de protection, que celui-ci soit activé par défaut sans intervention de l'utilisateur

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée



VI. LES FORMALITES OBLIGATOIRES EN CAS DE RESPONSABILITE CONJOINTE»

Afin d'éviter la situation où la multiplication du nombre de responsables d'un traitement peut provoquer une dilution des responsabilités, le Code a consacré son article 388 à la répartition des obligations entre responsables conjoints.

Cette disposition prévoit qu'en cas de responsabilité conjointe, les responsables conjoints doivent, d'un commun accord, « définir de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences de la loi » .

De manière transparente signifie que « les grandes lignes de l'accord [doivent être] mises à disposition de la personne concernée ». Cette formulation semble indiquer que les responsables conjoints n'ont pas l'obligation de communiquer activement à la personne concernée ces informations, mais simplement de les rendre disponibles, sur leur site internet respectif par exemple.

Indépendamment des termes de l'accord visé à l'alinéa 1 de l'Article 388 la personne concernée peut exercer les droits que lui confère les dispositions de la loi à l'égard de et contre chacun des responsables du traitement.



VI. LES FORMALITES OBLIGATOIRES EN CAS DE RESPONSABILITE CONJOINTE»

Si cet accord tend à régler la relation entre responsables conjoints, il n'est nullement opposable à la personne concernée qui reste parfaitement libre de faire valoir ses droits auprès du responsable du traitement de son choix, charge à eux de se coordonner et mettre en place les procédures nécessaires à un traitement efficace des demandes de ces personnes.



VII. ROLE DU SOUS-TRAITANT

Dans l'environnement des TIC, bien souvent les responsables de traitement font appel aux services de sociétés tierces pour leur permettre d'effectuer les traitements de données qu'ils souhaitent. Comme le dit l'adage, « la résistance d'une chaîne se mesure à son maillon le plus faible » d'où le recours à un sous-traitant doit également réglementé.

Si la quasi-totalité des obligations reposait sur le responsable du traitement, dorénavant, le sous-traitant assume personnellement une plus grande part de responsabilité dans les traitements auxquels il participe et doit dans certains cas lui aussi, comme le responsable du traitement, tenir un registre, nommer un DPO...

Le sous-traitant n'est plus vu comme un simple exécutant technique, mais comme un véritable partenaire du responsable du traitement, qui doit être associé à différents stades du traitement. Cette plus grande responsabilisation des sous-traitants s'explique en partie par le fait que les sous-traitants sont des entreprises parfois plus importantes que les responsables de traitement pour qui elles travaillent et sont parfois les seules à avoir l'expertise suffisante pour assurer une pleine effectivité aux dispositions du Code.

7.1 LE CHOIX DU SOUS-TRAITANT

Le responsable du traitement qui envisage de faire appel à un sous-traitant ne peut choisir le sous-traitant qu'il souhaite sans prendre certaines précautions au préalable. Il a le devoir de vérifier que celui-ci « présente des garanties suffisantes quant à la mise en oeuvre 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 de la personne concernée [Art. 388.1 du CDN]



VII. ROLE DU SOUS-TRAITANT

7.2. La relation entre le responsable du traitement et son sous-traitant [Art. 388.3 du CDN]

Le responsable du traitement et le sous-traitant sont tenus de conclure un contrat pour clarifier les droits et obligations de chacune des parties. Dans ce contrat, doivent notamment être précisés « 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, les obligations et les droits du responsable du traitement »

Le sous-traitant reste tenu par les informations qui lui ont été fournies par le responsable du traitement et n'a pas a priori à remettre en question la véracité de ces informations et la justesse de l'analyse quant à la nature des données traitées par exemple

Le contrat doit également mentionner une série d'obligations qui incombent au sous-traitant :



VII. ROLE DU SOUS-TRAITANT

- S'oblige à traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ». Cet engagement sera très souvent mentionné dans le contrat de travail des employés. Pour rappel, il est également tenu de mettre en place les mesures techniques et organisationnelles permettant d'éviter toute réutilisation de ces données ;
- S'oblige à prendre toutes les mesures requises afin de répondre à ses obligations en matière de sécurité et aider le responsable du traitement à garantir le respect de ses propres obligations compte tenu de la nature du traitement et des informations mises à la disposition du sous-traitant
- Aider le responsable du traitement dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes des personnes concernées qui le saisissent en vue d'exercer leurs droits. Il n'a donc pas l'obligation de répondre directement aux demandes des personnes concernées. En cas d'une pareille demande, il pourra éventuellement renvoyer au responsable du traitement qui est seul à même d'évaluer l'opportunité d'accéder à cette requête. Le sous-traitant n'est tenu que d'aider, techniquement, le responsable du traitement à faire droit à cette demande. Il commettrait selon nous une faute s'il donnait suite à une demande d'effacement, par exemple qui



VII. ROLE DU SOUS-TRAITANT

Le sous-traitant n'est tenu que d'aider, techniquement, le responsable du traitement à faire droit à cette demande. Il commettrait, selon nous, une faute s'il donnait suite à une demande d'effacement, par exemple qui lui serait directement adressée, sans au préalable avoir consulté le responsable du traitement. À tel point qu'il est probable que, dans ce cas, le responsable du traitement puisse se retourner contre son sous-traitant si cette initiative du sous-traitant lui était préjudiciable.

- Exécuter le choix du responsable du traitement de supprimer certaines données à caractère personnel ou les renvoyer à ce dernier, et détruire les copies existantes, sauf disposition légale imposant la conservation de celles-ci au terme de la prestation de services impliquant des traitements de données,



VII. ROLE DU SOUS-TRAITANT

- S'oblige à mettre à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues par la loi et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
- Informer immédiatement le responsable du traitement si, selon lui, une instruction de celui-ci constitue une violation de la loi ou d'autres dispositions du droit de la communauté par exemple relatives à la protection des données personnelles



JE VOUS REMERCIE