






DIRECTION DE LA DOCUMENTATION  
ET DES ARCHIVES

PLA

PLAN DE MISE EN CONFORMITE DES DONNEES A CARACTERE PERSONNEL DU TRESOR PUBLIC CONFORMEMENT A LA LOI N° 2013-450 DU 19 JUIN 2013 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL	Référence : DGTCP-DDA-PS4-PLA-461-2024
	Version 1 Date de rédaction : 31/10/2024 Page : 1/15

Objet : Ce document constitue le plan de mise en conformité des données à caractère personnel du Trésor Public.

Rédaction du document	Vérification du document	Validation du document
Monsieur DJEHI Yro Daniel Sous-Directeur de la Documentation Visa 	Madame LEGRE Evelyne Epse BERTE Directeur de la Documentation et des Archives Visa : 	DIRECTION GENERALE DU TRESOR ET DE LA COMPTABILITE PUBLIQUE Visa : 
Gestionnaire du document	Direction de la Documentation et des Archives	
Destinataires pour action	Destinataires pour information	Validité
DDA	- DGTCP - DSI - DSDI - DCRP - OED-TP - DRH	A Compter du : 03 -12- 2024



SOMMAIRE	Pages
SIGLES.....	4
GLOSSAIRE.....	5
I-CONTEXTE.....	8
II- CADRE LEGISLATIF ET REGLEMENTAIRE .....	9
III- CHAMP D'APPLICATION.....	10
IV-ETAPES DE MISE EN CONFORMITE DES DONNEES A CARACTERE PERSONNEL.....	10
IV-1- SENSIBILISATION / FORMATION DU PERSONNEL DE LA DGTCP..	10
IV-2- DESIGNATION D'UN CORRESPONDANT A LA PROTECTION.....	11
IV-3 - DIAGNOSTIC DES ACTIVITES ET PROCESSUS METIERS.....	13
IV-4- INVENTAIRE DES DONNEES A CARACTERE PERSONNEL ET CLASSIFICATION DES DONNEES TRAITEES.....	13
IV-5- ANALYSES DES CRITERES RELATIFS AUX DONNEES.....	13
IV-6-INVENTAIRE DES DONNEES TRAITEES Y COMPRIS LES TRANSFERTS DE DONNEES A L'ETRANGER.....	13



IV-7 IDENTIFICATION ET CLASSIFICATION DES SUPPORTS DE TRAITEMENT.....	14
IV-8- ANALYSE DES CRITERES DE CONSENTEMENT.....	14
IV-9- ANALYSE DES ECARTS.....	14
IV-10- PLAN D’ACTIONS CORRECTIVES.....	14
IV-11- AUTORISATION UNIQUE DE TRAITEMENT.....	15
IV-12- ATTESTATION DE CONFORMITE.....	15
IV-13- VEILLE REGLEMENTAIRE.....	15
V- DOCUMENTATION DE MISE EN CONFORMITE.....	15



## **SIGLES**

ARTCI : Autorité de Régulation des Télécommunication en Côte d'Ivoire

CAB : Cabinet

DGTCP : Direction Générale du Trésor et de la Comptabilité Publique

DDA : Direction de la Documentation et des Archives

DSI : Direction des Systèmes d'Informations

MFB : Ministère des Finances et du Budget

MPTIC : Ministère de la Poste et des Technologies de l'Information et de la  
Communication



## GLOSSAIRE

**Chiffrement** : Technique qui consiste à transformer des données numériques en un format intelligible en employant des moyens de cryptologie.

**Code de Conduite** : Charte d'utilisation élaborée par le responsable de traitement afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée et homologuée par l'Autorité de Protection.

**Courrier électronique** : Message sous forme de textes, de voix, de son ou d'image, envoyé par un réseau de communication publique, stocké sur un serveur de réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère.

**Cryptologie** : Science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non-répudiation.

**Destinataire d'un traitement des données à caractère personnel** : Toute personne habilitée à recevoir une communication de ces données, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données.

**Document** : Résultat d'une série de lettres, de caractères, de chiffres, de figures ou de tous autres signes ou symboles qui a une signification intelligible, quels que soient leur média et leurs modalités de transmission.

**Données** : Représentation d'une information dans un programme : soit dans le texte du programme (*code source*), soit en mémoire durant l'exécution. Les données, souvent codées, décrivent les éléments du logiciel tels qu'une entité, une interaction, une transaction, un événement, un sous-système, etc.



**Données à caractère personnel :** Information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

**Fichier de données à caractère personnel :** Ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé ou réparti de manière fonctionnelle ou géographique permettant d'identifier une personne déterminée.

**Information :** Élément de connaissance susceptible d'être présenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, etc.

**Responsable du traitement :** Personne physique ou morale, publique ou privée, 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.

**Signature électronique :** Donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

**Système d'information ou système informatique :** Dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou une partie de traitement automatisé de données en exécution d'un programme.

**Sous-traitant :** Personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable de traitement.



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



## I- CONTEXTE

Dans sa quête de performance en vue de « faire du Trésor Public, une Administration Excellente et intègre au service du Citoyen et des Parties Prenantes » le Trésor Public s'est tourné résolument vers la digitalisation de l'ensemble de ses Services. Ce qui facilite, dès lors, la naissance et la circulation d'un flux d'informations de toute nature, important pour le bon fonctionnement de l'ensemble de ses Services.

Au compte de ce réceptacle informationnel figurent en bonne et due forme les données à caractère personnel matérialisant les renseignements disponibles sur l'identification des acteurs en charge de la conduite de l'action administrative et des parties prenantes.

Définies selon la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel « comme toute information de quelque nature qu'elle soit indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique », les données à caractère personnel méritent une prise en charge efficiente. Celles-ci doivent faire l'objet de traitement pour en garantir une meilleure protection. Cela passe par la prise en compte des exigences législatives et réglementaires qui en définissent les étapes nécessaires à la mise en adéquation.

La loi n° 2013-450 du 19 Juin 2013 sus-citée en précise également les mécanismes opérationnels. Fort de cette exigence, le Trésor Public, Administration Publique certifiée ISO 9001 Version 2015, a inscrit la mise en conformité de ses Services à ladite loi.

Le document présentera la déclinaison opérationnelle de la mise en conformité en vue d'assurer la protection efficace des données à caractère personnel.



## **II- Cadre législatif et réglementaire**

### **Au niveau législatif**

- Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques.

### **Au niveau réglementaire**

- Décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire (ARTCI) ;
- Décret n°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;
- Décret n°2015-79 du 04 février 2015 fixant les modalités de dépôt des déclarations, de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel ;
- Arrêté n°511/MPTIC/CAB du 11 Novembre 2014 portant définition du profil et fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel ;
- Décision n°2017-0354 de l'Autorité de Protection de la République de Côte d'Ivoire du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.



### III- DOMAINE D'APPLICATION

Ce plan de conformité couvre les données à caractère personnel des clients internes et externes du Trésor Public.

### IV- ETAPES DE MISE EN CONFORMITE DES DONNEES A CARACTERE PERSONNEL

La décision n° 2017-0354 de l'Autorité de Protection de la République de Côte d'Ivoire du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel précise les différentes étapes de la mise en conformité.

Elles sont décrites comme suit :

#### **IV-1- Sensibilisation / Formation du personnel de la Direction Générale du Trésor et de la Comptabilité Publique**

Le personnel doit être sensibilisé et formé à :

- la protection de ses propres données ;
- la gestion et à la protection appropriée des données à caractère personnel qu'il manipule dans le cadre des activités professionnelles.

Pour ce faire, le Trésor Public doit mettre en place un programme de sensibilisation des utilisateurs et gestionnaires des données à caractère personnel. La collecte des données à caractère personnel doit désormais se faire avec le consentement de la personne concernée.

Aussi, la Direction de la Documentation et des Archives en collaboration avec la Direction de la Formation, doit-elle établir un programme de sensibilisation et de formation de l'ensemble du personnel du Trésor Public.



#### IV-2- Désignation d'un Correspondant à la protection

Le Correspondant à la protection est la personne physique ou morale chargée du traitement à l'effet de veiller d'une manière indépendante au respect des obligations prévues pour la protection des données à caractère personnel, par la législation en vigueur.

Il est l'interface entre :

- le responsable du traitement et l'Autorité de Protection ;
- le responsable du traitement et les personnes concernées.

##### • Profil du Correspondant à la protection

Son profil est défini par l'article 4 de l'arrêté n°511/MPTIC/CAB du 11 novembre 2014 portant définition du profil et fixant les conditions d'emploi du Correspondant à la protection des données à caractère personnel.

Pour les personnes physiques :

- être de nationalité ivoirienne ;
- avoir au minimum le niveau BAC+4 dans le domaine des sciences juridiques ou un niveau équivalent en informatique ou dans le domaine des réseaux et télécommunication/TIC ;
- avoir au moins cinq années d'expérience professionnelle dans les domaines de compétence évoqués ci-dessus ;
- avoir une compétence avérée en matière de protection des données à caractère personnel ;
- avoir une bonne connaissance des systèmes de gestion et d'exploitation des bases de données, des modes de stockage de données, des politiques de sécurité des systèmes d'information ;
- maîtriser les outils bureautiques et l'internet ;
- avoir d'excellentes capacités relationnelles et organisationnelles ;



- n'avoir jamais fait l'objet d'une condamnation pénale devenue définitive ou d'une interdiction définitive ou temporaire d'exercer une activité prononcée par une juridiction ivoirienne ou étrangère, ou encore de sanctions prononcées par l'Autorité de protection.

Le Correspondant à la protection des données à caractère personnel, personne physique ne peut être désigné que par un seul responsable de traitement et n'exerce ses missions qu'auprès de ce dernier sous peine de déchéance prononcée par l'Autorité de protection.

- **Les missions du Correspondant à la protection des données à caractère personnel sont définies par l'article 10 du même texte.**

Selon l'article 10 du texte susvisé, dans le cadre de ses missions, le Correspondant à la protection des données à caractère personnel accomplit les tâches suivantes :

- tenir à jour la liste des traitements effectués ;
- détenir une copie des codes et autres mots de passe par l'accès aux fichiers relatifs aux traitements effectués ;
- assurer l'accès à ses données à toute personne concernée qui en fait la demande en vue de l'exercice de ses droits reconnus par la législation en vigueur ;
- veiller au respect de la législation en matière de protection des données à caractère personnel ;
- signaler au responsable de traitement les violations constatées de la législation en matière de protection des données à caractère personnel ;
- notifier à l'ARTCI toute violation de la législation en matière de protection des données à caractère personnel préalablement signalée et non corrigée dans un délai de trois mois à compter du signalement.



#### **IV-3- Diagnostic des activités et processus métiers**

Un projet de mise en conformité commence toujours par un état des lieux.

Un diagnostic des activités de l'ensemble des Services du Trésor Public est à effectuer afin d'identifier celles et ceux qui sont liés au traitement des données à caractère personnel.

Il s'agira en relation avec la Direction des Systèmes d'Information (DSI) et la Direction des Ressources Humaines (DRH), de recenser tous les traitements de données effectués par l'ensemble des Services de la Direction Générale du Trésor et de la Comptabilité Publique.

A cet effet, un questionnaire doit être élaboré et adressé à l'ensemble des Services du Trésor Public en vue de collecter les informations.

#### **IV-4- Inventaire des données à caractère personnel et classification des données traitées**

Les données à caractères personnel traitées par le responsable du traitement sont inventoriées, puis classifiées selon les catégories définies par la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (données sensibles, données financières, données de localisation, etc.).

#### **IV-5- Analyse des critères relatifs aux données**

Les données seront analysées, afin de vérifier qu'elles obéissent aux critères définis par la loi. L'analyse consistera à vérifier que les données sont adéquates, pertinentes, limitées, exactes et tenues à jour, au regard des finalités pour lesquelles elles sont traitées.

#### **IV-6- Inventaire des données traitées y compris les transferts de données à l'étranger**

Les traitements seront identifiés et listés. Une description brève doit en être faite avec précision de leur finalité, des catégories de personnes concernées.



De même, les données transférées à l'étranger seront listées en précisant les destinataires, le pays de destination, le cadre de protection des données à caractère personnel de ce pays.

#### **IV-7- Identification et classification des supports de traitement**

Les supports de traitement devront être identifiés et classifiés, selon que les traitements sont manuels ou automatisés.

#### **IV-8- Analyse des critères de consentement**

Les données traitées devront être analysées pour évaluer la nécessité du consentement des personnes concernées. Cette analyse consiste donc à :

- identifier les cas d'exonération du consentement préalable des personnes concernées ;
- identifier les cas nécessitant le consentement des personnes concernées ;
- vérifier que le consentement préalable des personnes concernées est libre, spécifique, éclairé et univoque.

#### **IV-9- Analyse des écarts**

L'analyse des écarts sera effectuée sur l'information (finalités, destination...), l'appropriation, le droit d'accès et de rectification des personnes concernées, et sur le niveau de protection des données à caractère personnel traitées et des supports de traitement.

#### **IV-10- Plan d'actions correctives**

Un plan d'actions correctives des écarts décelés devra être défini en relation avec l'Autorité de protection aux fins de sa mise en œuvre par le responsable du traitement.



#### **IV-11- Autorisation unique de traitement**

En application du décret n°2015-79 du 04 février 2015 fixant les modalités de dépôt des déclarations de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel, l'Autorité de protection délivrera une autorisation pour l'ensemble des traitements effectués par le responsable du traitement.

Elle est soumise au paiement des frais d'autorisation dont devra s'acquitter l'organisme intéressé.

#### **IV-12- Attestation de conformité**

Après correction des écarts constatés, l'Autorité de protection délivrera une attestation de conformité au responsable du traitement du Trésor Public.

#### **IV-13- Veille règlementaire**

Pour toutes les nouvelles activités ou pour toutes les nouvelles données à caractère personnel traitées dans les activités identifiées, une analyse devra être effectuée afin de définir les exigences de conformité et de déclaration auprès de l'Autorité de Protection.

En plus des étapes énoncées ci-dessus, le responsable du traitement devra disposer d'une documentation afin d'être en conformité.

#### **V-Documentation de mise en conformité**

Le responsable de traitement doit démontrer la conformité à la protection des données à caractère personnel en apportant la preuve documentaire de l'ensemble des procédures mises en place.

C'est le principe de la responsabilité. Il s'agit de responsabiliser le Trésor Public et de l'inciter à s'engager à respecter le cadre légal en vigueur.