

**DECISION N°2022-0742**  
**DE L'AUTORITE DE PROTECTION**  
**DE LA REPUBLIQUE DE COTE D'IVOIRE**  
**EN DATE DU 5 JUILLET 2022**  
**PORTANT AUTORISATION DE TRAITEMENT**  
**DE DONNEES A CARACTERE PERSONNEL**  
**PAR VERSUS BANK**  
**(VIDEOSURVEILLANCE)**

## L'AUTORITE DE PROTECTION,

- Vu le règlement n°15/2002/CM/UEMOA du 23 mai 2002 relatif aux systèmes de paiement dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA)
- Vu la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Vu la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- Vu la loi n°2013-546 du 30 juillet 2013 relative aux Transactions électroniques ;
- Vu la loi n°2014-136 du 24 mars 2014 portant réglementation des bureaux d'information sur le crédit ;
- Vu la loi n°2016-992 du 14 novembre 2016 relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme ;
- Vu l'ordonnance n°2009-385 du 1<sup>er</sup> décembre 2009 portant réglementation bancaire ;
- Vu l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;
- Vu le décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;
- Vu le décret n°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;
- Vu le 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 ;
- Vu le 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 ;
- Vu le décret n°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;
- Vu le décret n°2019-947 du 13 novembre 2019 portant nomination du Président de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

- Vu le décret n°2019-985 du 27 novembre 2019 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;
- Vu le décret n°2022-265 du 13 avril 2022 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;
- Vu 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 ;
- Vu la décision n°2013-0003 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 20 septembre 2013 portant règlement intérieur ;
- Vu la décision n°2014-0020 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant adoption des règles de conduites relatives au traitement et à la protection des données à caractère personnel (DCP);
- Vu la décision n°2014-0021 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel ;
- Vu la décision n°2014-0022 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions de la suppression des liens vers les données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;
- Vu la décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;
- Vu la Décision n°2017-353 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant vérification préalable ;
- Vu la décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date 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 ;
- Vu la décision n°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

Vu la décision n°2020-0581 de l'Autorité de protection de la République de Côte d'Ivoire en date du 30 juillet 2020 fixant les critères et les conditions d'exercice des activités de :

- correspondant à la protection des données, personne morale ;
- audit de conformité ;
- formation

Vu la décision n°2021-0629 de l'Autorité de protection de la République de Côte d'Ivoire en date du 23 Février 2021 portant autorisation de traitement de données à caractère personnel par VERSUS BANK ;

Vu la décision n°2021-0676 de l'Autorité de protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel ;

**Par les motifs suivants :**

**- Sur la compétence de l'Autorité de Protection**

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par **VERSUS BANK** sise à Abidjan, Plateau, Boulevard Botreau Roussel, Avenue Joseph Anoma, Immeuble Crrae-Uemoa01 BP 2056 Abidjan 01, téléphone 27 20 25 60 99, immatriculée au numéro 096/MEMI/DGAT/DAG/SDVA du 16 Février 2012.

Considérant que **VERSUS BANK est une entreprise exerçant dans le domaine bancaire.**

Considérant que l'article 47 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, dispose que l'Autorité de protection est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitement des données à caractère personnel ;

Dès lors l'Autorité de Protection est compétente, pour examiner la demande d'autorisation de traitement initiée par **VERSUS BANK** ;

**- Sur la recevabilité de la demande d'autorisation**

Considérant qu'aux termes de l'article 7 de la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le traitement portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphone, le traitement des données à caractère personnel comportant des données biométriques sont soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant qu'en l'espèce, **VERSUS BANK** envisage de collecter, et de stocker les données à caractère personnel, tels que, les numéros de plaques d'immatriculations, et les données biométriques, notamment les images et, les mouvements de toutes personnes à l'intérieur et aux alentours de son siège social ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la 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 ;

Considérant qu'en l'espèce, **VERSUS BANK** a décidé de mettre en place un système de vidéosurveillance en vue d'assurer la sécurité des biens et des personnes au sein de sa structure ;

Que pour ce faire, elle a décidé de collecter et de traiter les données à caractère personnel des visiteurs et des membres de son personnel ;

L'Autorité de Protection en conclut que **VERSUS BANK** a qualité de Responsable du traitement ;

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection, à la confidentialité des données traitées et à la fonction de la personne ou le service auprès duquel s'exercent les droits des personnes concernées ;

Qu'en l'espèce, la demande d'autorisation de **VERSUS BANK** contient les mentions minimums prescrites par l'article 9 précité ;

Considérant qu'au regard de tout ce qui précède, ladite demande satisfait les conditions de formes exigées par les articles 7 et 9 de la loi n°2013-450 relative à la protection des données à caractère personnel ;

L'Autorité de Protection déclare que la demande de **VERSUS BANK** est recevable en la forme.

#### - Sur la légitimité et la licéité du traitement

Considérant que conformément aux dispositions de l'article 14 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le traitement de données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable ;

Considérant que **VERSUS BANK** envisage de collecter et de stocker les données à caractère personnel des personnes présentes dans ses locaux et aux alentours, par le biais d'un système de vidéosurveillance ;

Considérant toutefois que **VERSUS BANK** n'apporte pas la preuve que les personnes concernées ont exprimé leur consentement préalable au traitement de leurs données ;

Considérant par ailleurs, que l'existence d'un système de vidéosurveillance doit être portée à la connaissance de toute personne filmée ou susceptible de l'être, de façon claire et permanente, par un pictogramme placé à hauteur de vue, dans les zones filmées par les caméras ;

Considérant en outre, que l'utilisation d'un système de vidéosurveillance au sein d'une entreprise est subordonnée à l'accord du personnel, qui doit exprimer clairement son consentement à son installation ;

L'Autorité de Protection prescrit à **VERSUS BANK** de mettre en place un processus de recueil individuel du consentement de son personnel ;

L'Autorité de Protection prescrit également à **VERSUS BANK**, d'informer les personnes concernées de l'existence du dispositif de vidéosurveillance, au moyen de pictogrammes placés de façon visible dans les zones sous surveillance.

#### - Sur la finalité

Considérant l'article 16 de la Loi relative à la protection des données à caractère personnel qui dispose que les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités ;

Considérant qu'en l'espèce, **VERSUS BANK** envisage la mise en place d'un système de vidéosurveillance, aux fins :

- d'assurer la sécurité des biens et des personnes ;
- d'anticiper et de réagir en cas d'incendies et accidents ;
- d'identifier les auteurs de vols, de dégradations ou d'agressions ;

L'Autorité de Protection considère que lesdites finalités sont déterminées, explicites et légitimes.

### - Sur la période de conservation des données traitées

Considérant que l'article 16 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que, les données traitées doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ;

Considérant qu'en l'espèce, **VERSUS BANK** a indiqué que les données traitées sont conservées pendant trente (30) jours avec recyclage automatique.

L'Autorité de protection considère que cette durée de conservation n'est pas excessive.

Toutefois, l'Autorité de Protection prescrit que les données traitées soient conservées pendant une durée de trente (30) jours, et en cas d'incidents, pendant une période d'un (01) an à compter de la dernière sauvegarde mensuelle des données traitées.

### - Sur la proportionnalité des données traitées

Considérant que selon les dispositions de l'article 16 de la loi n°2013-450 du 19 juin 2013, relative à la protection des données à caractère personnel, les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

Considérant qu'en l'espèce, **VERSUS BANK** indique que le traitement concerne les données suivantes :

- **Données d'identification** : les images des visiteurs et des membres de son personnel ;  
les numéros de plaque d'immatriculation, modèle et couleur des véhicules ;
- **Données de localisation** : les différents mouvements détectés par les caméras dans les lieux placés sous surveillance.

En conséquence, l'Autorité de Protection conclut que les données collectées sont pertinentes, adéquates et non excessives au regard des finalités.

### - Sur les destinataires ou catégories de destinataires habilités à recevoir communication des données

Considérant les dispositions de l'article 9 de la loi n°2013-450 relative à la protection des données à caractère personnel, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant que la visualisation des images doit être restreinte aux seuls destinataires habilités, en charge de la sécurité des locaux ou installations sous surveillance ;

Considérant en l'espèce que **VERSUS BANK** indique que les destinataires des données traitées sont les personnes en charge de la sécurité de la vidéosurveillance, à savoir :

- Le chef de service sécurité des systèmes d'information ;
- Le contrôleur informatique sénior, chargé de la sécurité des systèmes électroniques et données à caractère personnel ;
- Le contrôleur informatique.

Considérant que les destinataires susmentionnés sont les agents des services internes de **VERSUS BANK** ;

Qu'en l'espèce, **VERSUS BANK** n'a pas mentionné dans son formulaire de demande d'autorisation qu'elle effectuera un transfert de données ;

L'Autorité de Protection prescrit que lesdites données ne fassent l'objet d'aucun transfert, ni d'aucune communication aux services non habilités de **VERSUS BANK** :

L'Autorité de Protection autorise également que les données traitées soient communiquées, le cas échéant :

- aux agents assermentés et habilités de l'Autorité de Protection dans le cadre de leurs missions ;
- aux Autorités publiques ivoiriennes compétentes, par le biais de leurs agents habilités, agissant dans le cadre de leurs missions ;
- au Procureur de la République de Côte d'Ivoire ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire, munis d'une réquisition.

#### - **Sur la transparence des traitements**

Considérant qu'aux termes des articles 18 et 28 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la transparence implique l'information obligatoire et claire des personnes concernées par le responsable du traitement ;

Qu'il s'agit en l'espèce pour **VERSUS BANK** de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- de l'identité du responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- des finalités du traitement, des catégories de données concernées, des destinataires auxquels les données sont susceptibles d'être communiquées ;
- de l'existence et des modalités d'exercice de leurs droits d'accès et de rectifications,
- de la durée de conservation des données,
- de l'éventualité de tout transfert de données à destination de pays tiers ;

Considérant que les personnes concernées (salariés, clients, visiteurs etc.) doivent être clairement informées de l'existence d'un système de vidéosurveillance et des destinataires des informations traitées ;

Considérant que, **VERSUS BANK** indique que les personnes concernées sont informées de l'existence d'un système de vidéosurveillance par voie d'affichage ;

Considérant que le formulaire de demande d'autorisation indique qu'il existe des pictogrammes aux différents endroits où sont installées les caméras ;

Que les mentions devant figurer sur les pictogrammes n'ont pas été mentionnées dans le formulaire de demande d'autorisation.

L'Autorité de Protection prescrit à **VERSUS BANK de mentionner de façon claire et visible.**

les informations suivantes sur les différents pictogrammes:

- le nom du responsable de traitement ;
  - le fait que l'établissement est placé sous vidéosurveillance ;
  - la finalité de ce dispositif (la sécurité des biens et des personnes) ;
  - les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès, de rectification et d'opposition ;
  - le numéro de l'autorisation octroyée par l'Autorité de protection.
- 
- **Sur les droits d'accès direct, d'opposition, de rectification des personnes concernées**

Considérant que les articles 9 et 29 à 34 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel prescrivent que le responsable du traitement doit indiquer dans sa demande, la fonction de la personne ou le service auprès duquel s'exercent les droits reconnus aux personnes concernées, notamment les droits d'accès, de rectification, d'effacement ;

Considérant que **VERSUS BANK** indique que les droits d'accès, d'opposition, de rectification, de suppression et retrait du consentement, pourront être exercés auprès de son correspondant à la protection ;

L'Autorité de Protection considère que les dispositions relatives, à la désignation d'un correspondant à la protection pour l'exercice des droits d'accès direct, d'opposition, de rectification, des personnes concernées sont respectées.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique et logique ;

Considérant qu'au vu des éléments techniques fournis dans le formulaire de demande d'autorisation, le niveau de sécurité du système d'information de **VERSUS BANK** lui permet de mettre en œuvre la vidéosurveillance dans ses locaux et leurs alentours pour les finalités déclarées ;

Qu'il ressort des documents communiqués par VERSUS BANK, qu'elle a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données, conformément aux dispositions de l'article 41 de la Loi susmentionnée ;

L'Autorité de Protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

**Après en avoir délibéré,**

**DECIDE :**

**Article 1 :**

**VERSUS BANK** est autorisée à effectuer la collecte, l'enregistrement et le stockage des données à caractère personnel ci-après :

- les données d'identification : numéro de plaque d'immatriculation, modèle et couleur des véhicules;
- les données de localisation : les différents mouvements détectés par les caméras dans les lieux placés sous surveillance ;
- les données biométriques : images des personnes.

Les données visées au présent article concernent les employés et visiteurs de **VERSUS BANK**

**Article 2 :**

Les données traitées par **VERSUS BANK** ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de Protection.

**Article 3 :**

**VERSUS BANK** l'obligation de procéder au recueil du consentement préalable, formel des personnes concernées. Elle devra en fournir les preuves à l'Autorité de Protection.

**Les pictogrammes installés par VERSUS BANK**

doivent indiquer, d'une façon claire et visible, les informations suivantes :

- le nom du responsable de traitement,
- le fait que l'établissement est placé sous vidéosurveillance ;
- la finalité de ce dispositif (la sécurité des personnes et des biens) ;
- les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès de rectification et d'opposition
- le numéro de l'autorisation octroyée par l'Autorité de Protection.

#### Article 8 :

Le correspondant à la protection désigné par **VERSUS BANK** tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

#### Article 9 :

**VERSUS BANK** veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel.

**VERSUS BANK** est tenue de mettre en place:

- un dispositif de formation de son correspondant à la protection et de ses agents habilités .
- un dispositif de sensibilisation de son personnel.

La formation devra être sanctionnée par un certificat ou une attestation de formation.

#### Article 10 :

**VERSUS BANK** veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, **VERSUS BANK** doit s'assurer que, ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à **VERSUS BANK** ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

**VERSUS BANK** est tenu de :

- s'assurer de la viabilité et de la sécurité du réseau de transmission en vue de garantir la sécurité de la vie privée des personnes prises en images ;
- veiller à la sécurité du disque dur chargé de stocker les images et du système d'exploitation ;
- veiller à la mise à jour du système d'exploitation et les applications qui y sont installées afin de conserver et de garantir la sécurité.

#### Article 11 :

Conformément à l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, **VERSUS BANK** est tenue d'établir pour le compte de l'Autorité de Protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

**VERSUS BANK** communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

**Article 12 :**

L'Autorité de Protection procède à des contrôles auprès de VERSUS BANK, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la réglementation en vigueur.

**Article 13 :**

La présente décision entre en vigueur à compter de la date de sa notification à VERSUS BANK

**Article 14 :**

Le Directeur Général est chargé de l'exécution de la présente décision, qui sera publiée au Journal Officiel de la République de Côte d'Ivoire et sur le site internet de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire.

Fait à Abidjan, le 05 Juillet 2022  
En deux (2) exemplaires originaux

Le Président



**Dr Coty Souleïmane DIAKITE**  
COMMANDEUR DE L'ORDRE NATIONAL

