africa *data protection*

Newsletter n°3 - Juin 2023

4 amendes prononcées au cours de ces derniers mois

Une plainte contre TikTok a été déposée devant la CDP au Sénégal

L'autorité ougandaise de protection des données publie un rapport sur la formation des délégués à la protection des données

2 NOUVEAUX PAYS AFRICAINS SE DOTENT DE LOIS DEDIÉES À LA PROTECTION DES DONNÉES

Édito

Jules Hervé Yimeumi
Juriste Délégué à la Protection des Données

Au cours de ces derniers mois, la protection des données à caractère personnel a beaucoup évolué en Afrique. Plusieurs points ont marqué cette évolution. Tout d'abord, au Nigéria, la Chambre des représentants a annoncé sur Twitter, le 24 mai 2023, que le projet de loi nigérian sur la protection des données avait passé sa troisième lecture après son adoption au Sénat nigérian. Ce projet de loi décrit les exigences pour les responsables de traitement, telles que la notification de violation des données, la réalisation d'Analyses d'Impact relatives à la Protection des Données (AIPD), la nomination d'un délégué à la protection des données et les droits des personnes concernées. À noter que le Nigéria dispose actuellement d'un règlement sur la protection des données daté de 2019 et que le Nigeria Data Protection Bureau (NDPB) est l'autorité de protection des données.

Ensuite, en République Démocratique du Congo (RDC) , un code du numérique a été promulgué le 13 mars 2023. Ce code établit un encadrement juridique complet de l'économie numérique.

Édito

Au sein de ce code (voir schéma ci-dessous), le titre III (contenu dans le Livre III) fait un focus sur la donnée personnelle. Le titre IV, lui, crée l'Autorité de Protection des Données (APD).

DES ACTIVITÉS ET SERVICES NUMÉRIQUES — LIVRE I

LIVRE II — **DES ÉCRITS, OUTILS ÉLECTRONIQUES ET DES PRESTATAIRES DE SERVICES DE CONFIANCE**

DES CONTENUS NUMÉRIQUES — LIVRE III

TITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION
TITRE II : DES CONTENUS PUBLICS
TITRE III : DES DONNÉES PERSONNELLES
TITRE IV : DE L'AUTORITÉ DE PROTECTION DES DONNÉES

LIVRE IV — **DE LA SÉCURITÉ ET DE LA PROTECTION PÉNALE DES SYSTÈMES INFORMATIQUES**

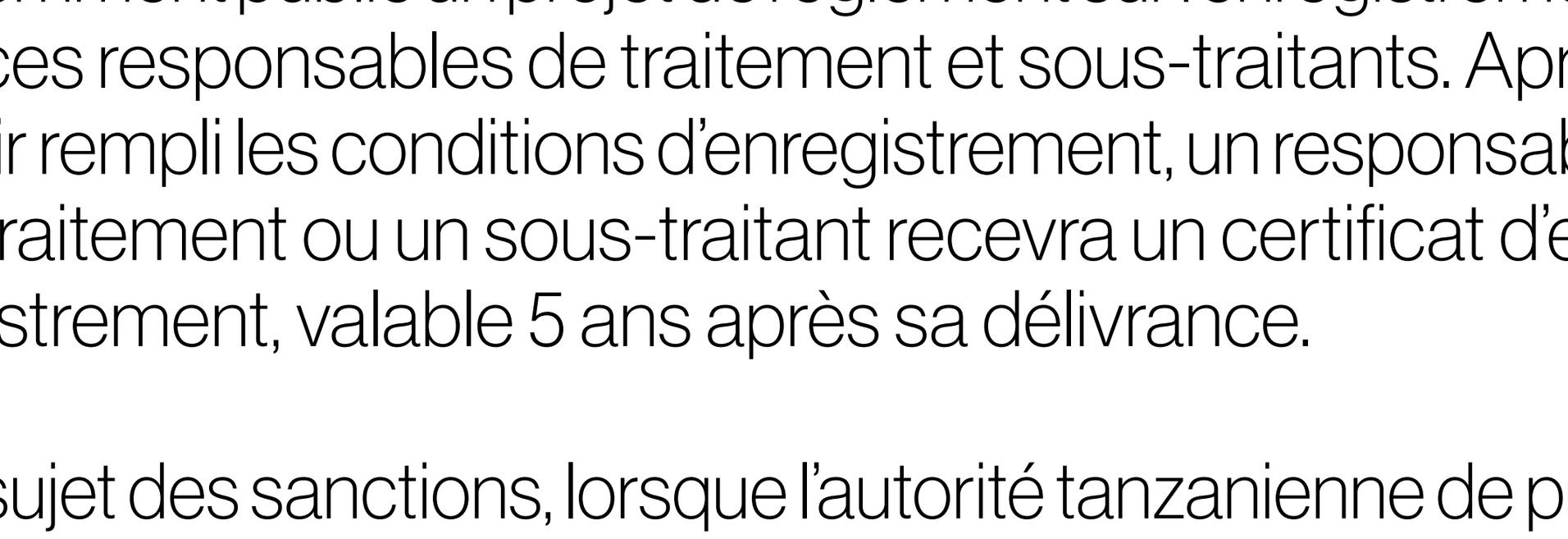
DES DISPOSITIONS DIVERSES, TRANSITOIRES, ABROGATOIRES ET FINALES — LIVRE V

Livres contenus dans la code du numérique en RDC avec un focus sur le livre III

Concernant les sanctions, lorsque qu'un responsable de traitement ne se conforme pas aux dispositions de ce Livre III, l'APD peut lui infliger une amende pouvant atteindre 5% de son chiffre d'affaires annuel, hors taxe de l'exercice écoulé, si la violation a conduit à la mort ou tentative de meurtre d'une ou plusieurs personnes.

En outre, c'est en Tanzanie qu'une loi sur la protection des données personnelles est entrée en vigueur le 1er mai 2023, soit cinq mois après son adoption par le Parlement.
Cette loi, comme de nombreuses autres lois africaines sur la protection des données, exige que les responsables de traitement et les sous-traitants s'enregistrent auprès de l'autorité de protection des données avant de collecter ou traiter des données personnelles (article 14).
Le Ministre de la Communication tanzanien a, qui plus est, récemment publié un projet de règlement sur l'enregistrement de ces responsables de traitement et sous-traitants. Après avoir rempli les conditions d'enregistrement, un responsable de traitement ou un sous-traitant recevra un certificat d'enregistrement, valable 5 ans après sa délivrance.

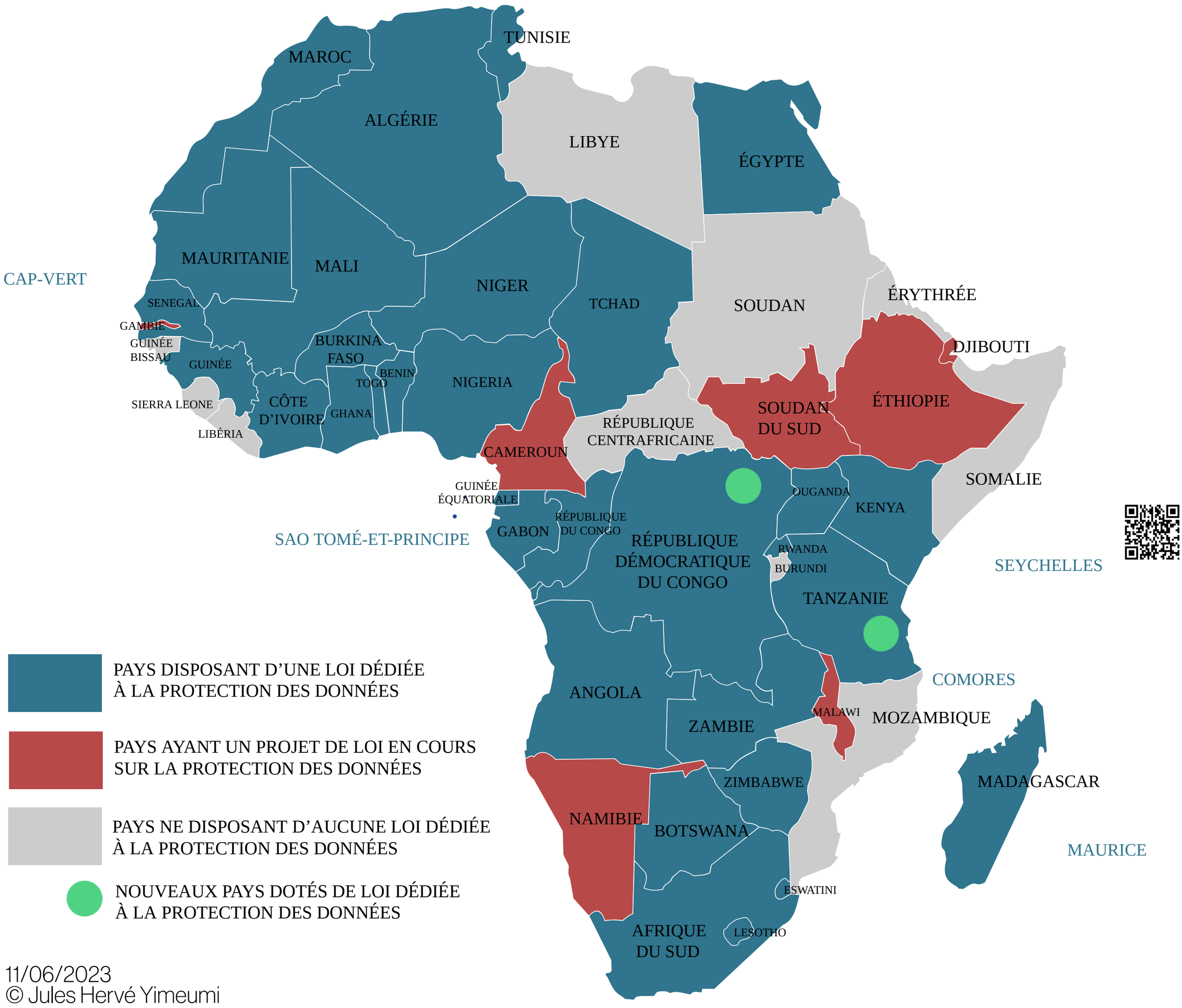
Au sujet des sanctions, lorsque l'autorité tanzanienne de protection des données décide d'en émettre, la loi fixe l'amende maximale à environ 41 320 euros.



Comparaison de la validité des certificats en Tanzanie et au Kenya

Édito

La cartographie ci-dessous fait un état des lieux des pays disposant ou non d'une loi dédiée à la protection des données.



11/06/2023
© Jules Hervé Yimeumi

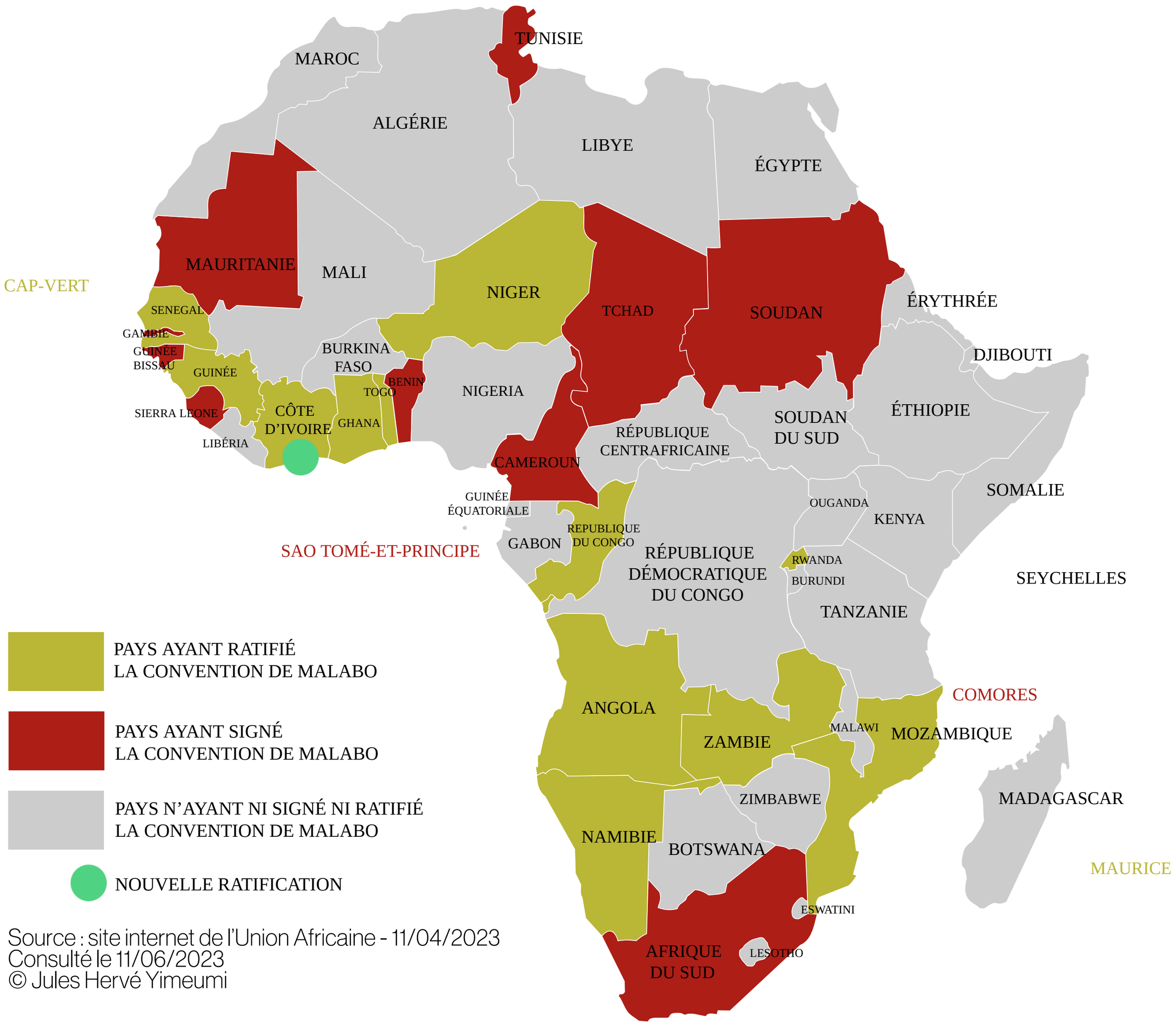
Etat des lieux des pays disposant ou non d'une loi dédiée à la protection des données

A l'échelle continentale, la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel (convention de Malabo) devrait entrer en vigueur dans quelques semaines.

En effet, 14 pays africains ont déjà ratifié la convention de Malabo et conformément à l'article 36 de la Convention, 15 ratifications sont nécessaires pour que la convention entre en vigueur. La RDC fait partie des pays ayant ratifié la convention mais elle ne figure pas encore sur la liste de l'Union Africaine. Elle devrait apparaître lors de la prochaine mise à jour de la liste des pays ayant ratifié la convention.

Édito

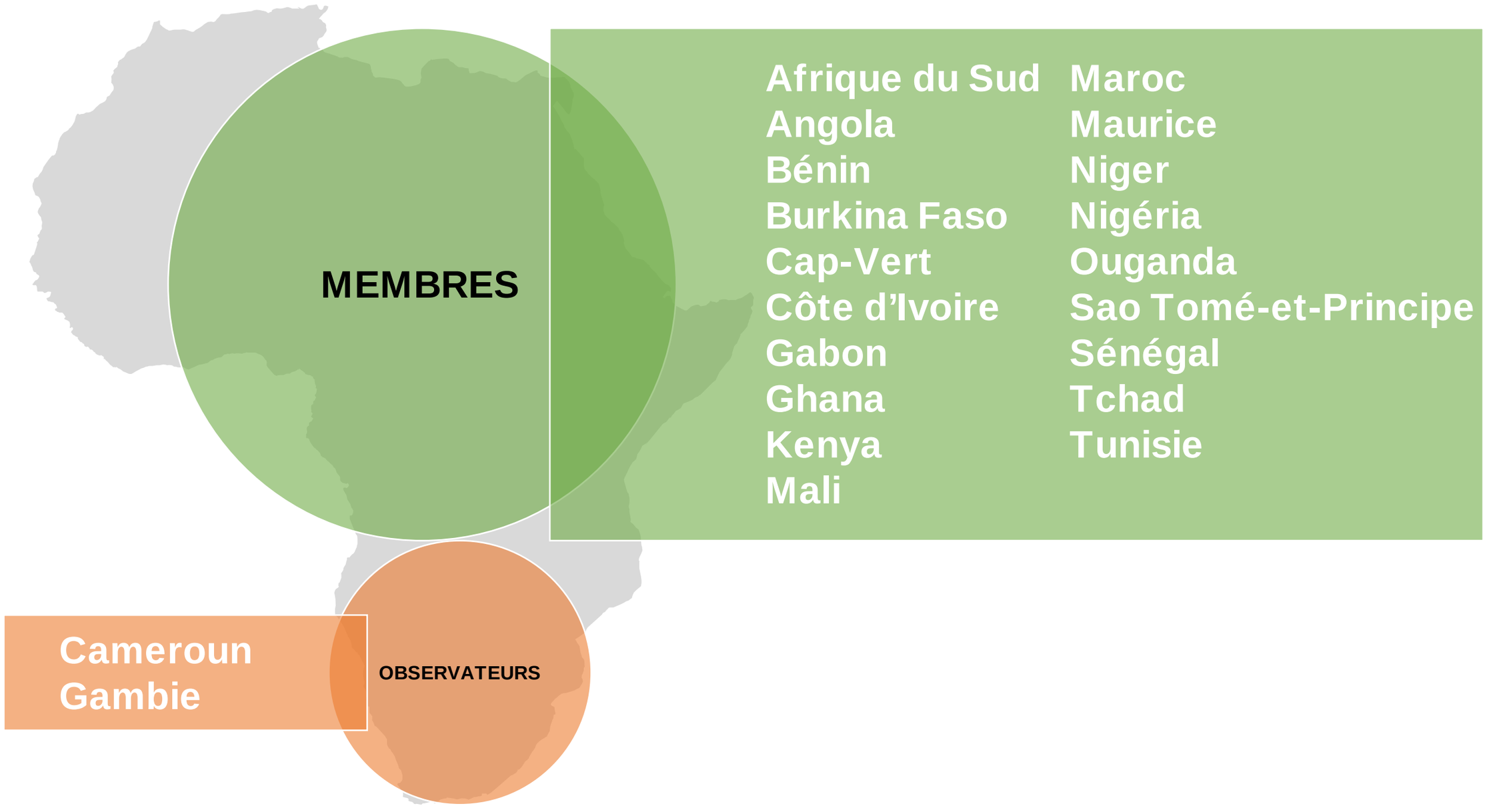
Ci-dessous, cette cartographie mise à jour présente des pays ayant signé et ratifié la convention de Malabo.



Source : site internet de l'Union Africaine - 11/04/2023
Consulté le 11/06/2023
© Jules Hervé Yimeumi

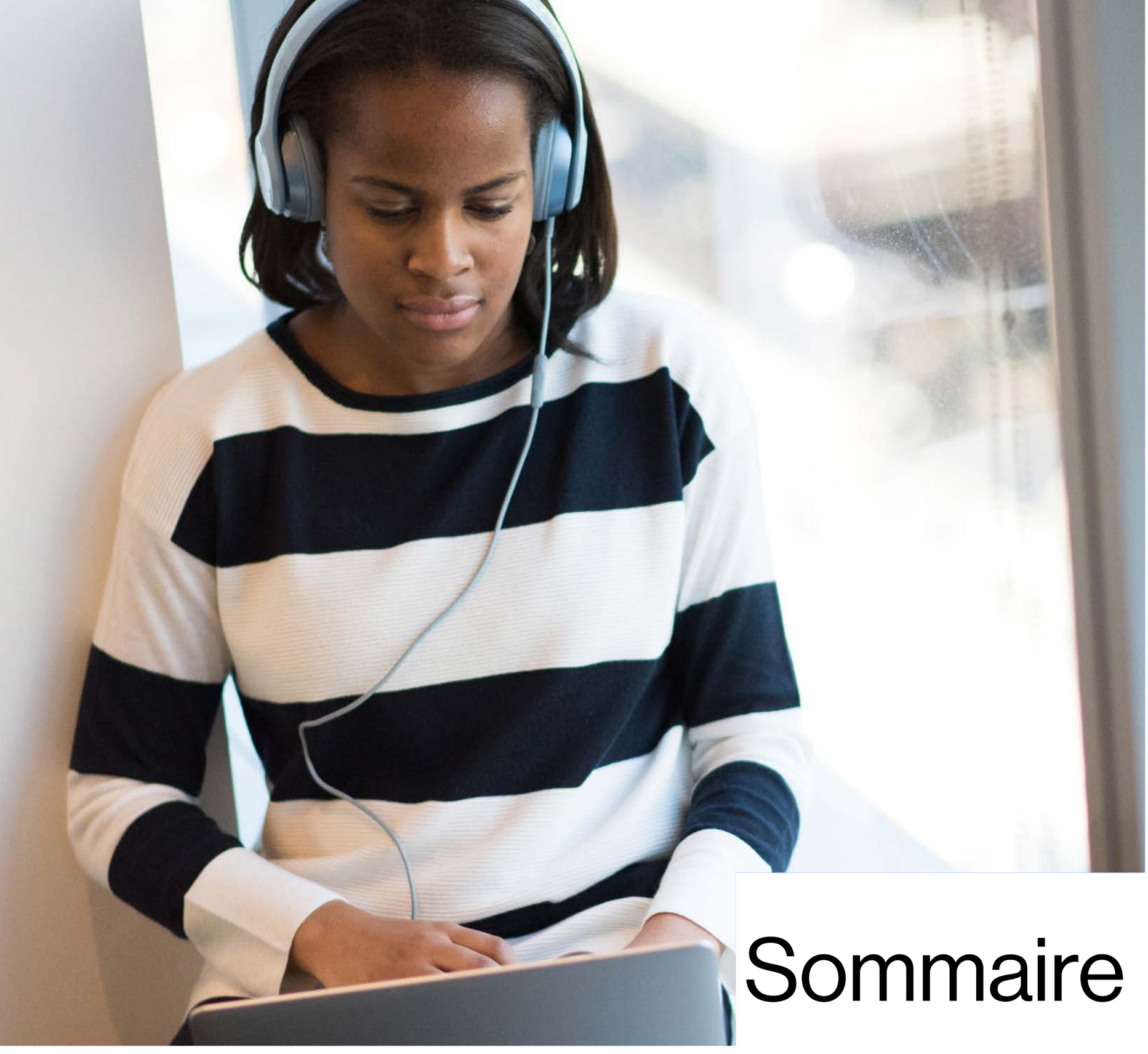
Pays ayant signé et ratifié la convention de l'UA sur la cybersécurité et la protection des données à caractère personnel (convention de Malabo)

Enfin, le Réseau Africain des autorités de Protection des Données Personnelles (RAPDP) s'est réuni dans la capitale burkinabé, du 8 au 13 Mai 2023, pour échanger sur les nouveaux enjeux de la protection des données et tenir la 6ème assemblée générale du Réseau. Pendant quatre jours, les autorités de protection ont discuté des questions qui touchent leur secteur, notamment des nouveaux défis comme l'Intelligence artificielle, l'identité numérique, les données des personnes en déplacement, les données de santé, la gestion des plaintes, la relation avec les GAFAM et la régulation des réseaux sociaux.



Membres et observateurs du RAPDP

A la fin des travaux, un nouveau bureau a été élu : ainsi, le Niger, à travers la présidente de la Haute Autorité de Protection des Données Personnelles (HAPDP), a été porté à la tête du RAPDP. Le Kenya et l'Angola occupent respectivement la 1 ère et la 2eme vice-présidence. Le Maroc assure toujours le Secrétariat Permanent du Réseau.

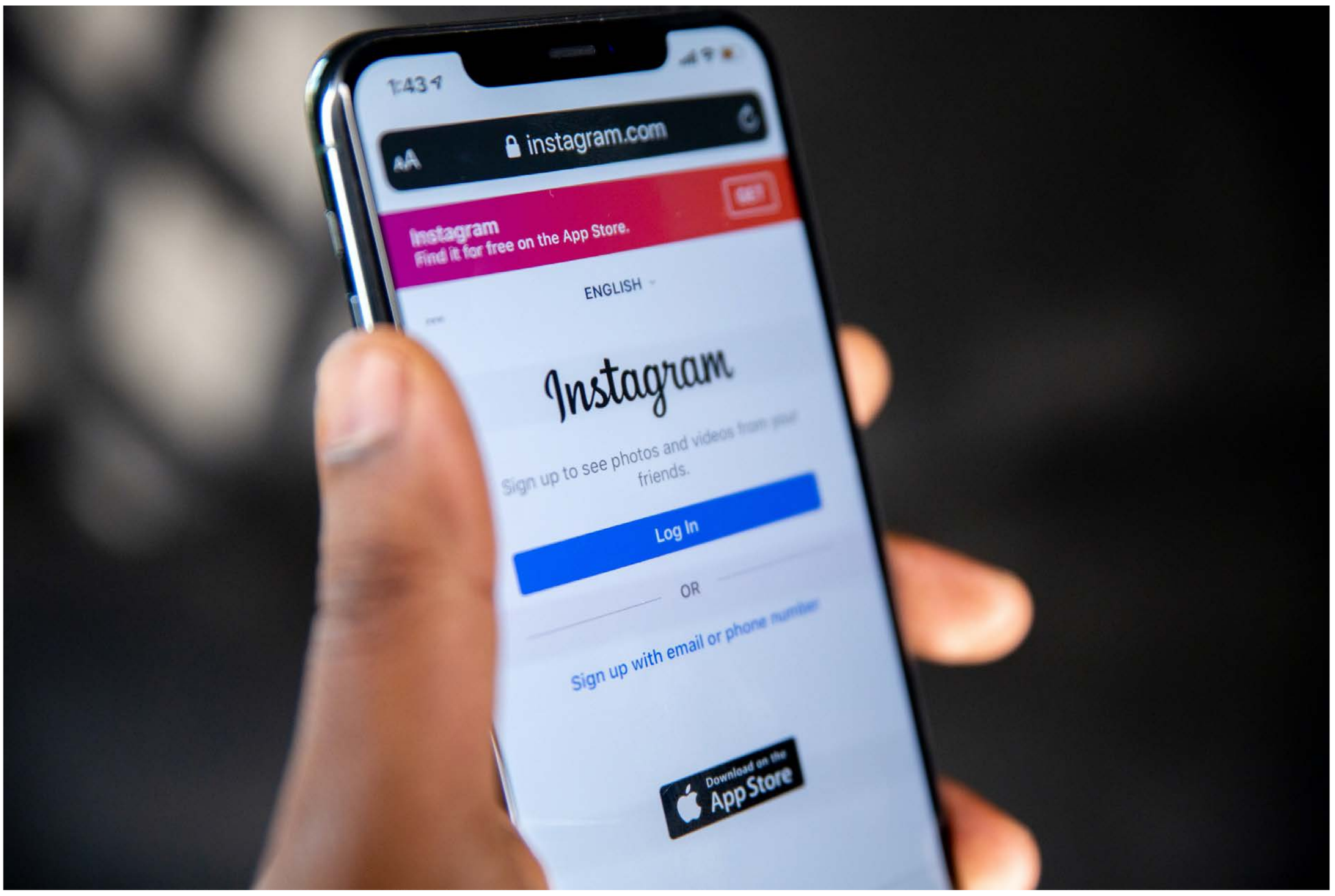


© Unsplash

Sommaire

Kenya : l'ODPC inflige trois amendes à des organismes

Au cours de ces derniers mois, L'Office of the Data Protection Commissioner (ODPC), a infligé trois amendes à 3 organisations. La première sanction concerne OPPO. L'ODCP a émis un avis d'exécution à l'encontre de la marque de smartphones, pour avoir porté atteinte à la vie privée d'un plaignant en utilisant sa photo sur le compte Instagram (stories) de l'entreprise sans son consentement. L'avis de sanction d'une amende de 33 500 € a été émis conformément à loi «Data Protection Act» (2019) et au règlement «Data Protection Regulations» (2021).



© Unsplash

Malgré cet avis d'exécution, Oppo Kenya a refusé de coopérer avec l'ODPC. La marque n'a pas présenté et/ou élaboré de politique de conformité, conformément à l'article 37 de la loi sur la protection des données. De plus, Oppo Kenya n'a pas présenté de politique de protection des données conforme à l'avis d'exécution émis. Enfin, la marque n'a pas non plus prouvé qu'elle avait mis en place un mécanisme de réclamation interne pour traiter les plaintes des personnes concernées. En conséquence, Oppo Kenya s'est vu infliger cette amende.

Concernant les deux autres sanctions, l'ODPC a émis deux avis de sanction à l'encontre de «Whitepath Company Limited» et de «Regus Kenya» pour la non-application de la loi de protection des données et des manquements à l'obligation de réponse aux notifications de plainte. Ces entreprises ont été sommées de payer chacune la somme d'environ 33 500 €. L'entreprise «Ecological Industries Limited» a, quant à elle, reçu une injonction d'application de la loi pour avoir refusé de coopérer suite à plusieurs plaintes déposées contre elle pour l'utilisation illégale des photos des plaignants.

Dans le communiqué de presse au sujet de la sanction d'OPPO, la commissaire à la protection des données, Immaculate Kassait, MBS, a exhorté toutes les organisations à se conformer à la loi sur la protection des données en mettant en œuvre des principes et des garanties pour toutes les activités de traitement liées à la collecte et au stockage des données personnelles.

© Unsplash

« L'ODPC demande instamment aux responsables du traitement et aux sous-traitants de veiller à ce que le traitement des données personnelles soit conforme aux dispositions de la loi. Le non-respect de la loi entraînera la mise en place de procédures de sanctions », a-t-elle souligné.

L'autorité ougandaise de protection des données publie un rapport sur la formation des DPO

© Unsplash

Le Personal Data Protection Office (PDPO), l'autorité Ougandaise de protection des données, a publié son rapport d'évaluation des besoins de formation des délégués à la protection des données (DPO). Le rapport précise que le PDPO a mené une enquête d'évaluation auprès des 510 délégués à la protection des données désignés par les entités enregistrées à compter du 13 octobre 2022, afin d'établir les lacunes dans les compétences requises par les DPO pour effectuer des tâches liées à la conformité. Plus précisément, l'évaluation visait, entre autres, à identifier le niveau d'implication des DPO dans la gouvernance des activités de protection des données et de la vie privée, et à déterminer si les DPO élaboraient et mettaient en œuvre des programmes de protection des données et de sensibilisation à la vie privée, en vertu de la loi sur la protection des données et la vie privée de 2019.

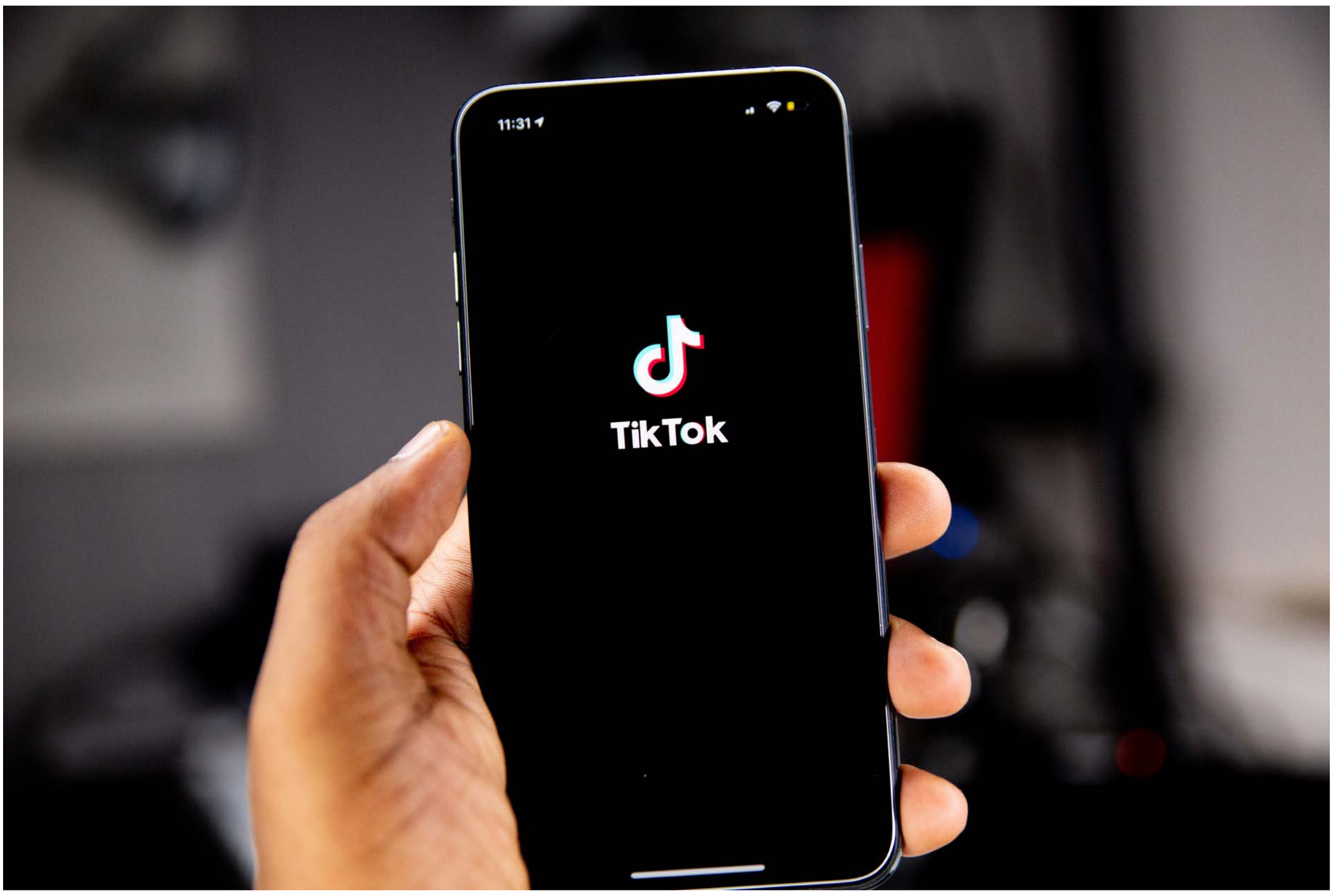
Ainsi, le rapport souligne que presque tous les DPO évalués n'avaient aucune certification en matière de protection des données, que la plupart d'entre eux avaient des connaissances

limitées sur la façon de développer et de mettre en œuvre un programme de gestion de la vie privée et que la majorité n'avait pas été impliquée dans la conduite de l'analyse d'impact relative à la protection des données. À la lumière de ce qui précède, le PDPO a encouragé les DPO à se former et à obtenir des certifications, et leur a recommandé de se concentrer sur les domaines suivants :

1. **L'élaboration et la mise en œuvre de politiques et de procédures sur la protection des données et de la vie privée**
2. **La sécurité des informations**
3. **La gestion des durées de conservation et les politiques de confidentialité**
4. **L'élaboration et la mise en œuvre d'un programme de sensibilisation et de formation**
5. **La gestion des violations des données personnelles et le traitement des plaintes**
6. **La réalisation des audits de protection des données et de la vie privée et la réalisation d'analyse d'impact (AIPD)**
7. **Le privacy by design et le privacy by default**
8. **La compréhension des mécanismes de transferts transfrontaliers de données**

Enfin, le rapport ajoute que le PDPO devrait élaborer et publier des notes d'orientation, relatives, d'une part, à la désignation d'un DPO, en mettant en évidence les compétences nécessaires pour remplir le rôle et, d'autre part, aux mécanismes de transferts transfrontaliers de données.

Une plainte contre TikTok a été déposée devant la CDP au Sénégal



© Unsplash

Le Rassemblement des Entreprises du secteur TIC (Restic) a décidé de porter plainte contre TikTok pour non-respect de la législation sur les données personnelles des enfants et des mineurs. Dans une interview accordée à Radio France Internationale, le secrétaire général exécutif du Restic, Moustapha Diakhaté, a expliqué que le développement de TikTok au Sénégal, un marché en pleine croissance, était inquiétant.Pour le Restic, les contenus problématiques sont : les contenus violents, à caractère sexuel ou obscènes, voire, tout simplement « bannis par nos us et coutumes, ici au Sénégal et en Afrique ».

Diakhaté a souligné que TikTok était loin d'être le seul réseau social à recueillir des données sur les utilisateurs africains, mais qu'il était le plus rapide en termes de croissance. Le Restic souhaite que TikTok clarifie ses mécanismes de stockage de données et que les autorités sénégalaises puissent y avoir accès pour garantir que les données ne soient pas utilisées à d'autres fins que celles pour lesquelles elles ont été initialement collectées.

L’autorité angolaise de protection des données inflige une amende de 140 000 euros à Africell

L’Agência de Protecção de Dados (APD), l’autorité angolaise de protection des données a infligé une amende de 140 000 euros à Africell pour violation de la loi sur la protection des données personnelles. Selon la délibération de l’APD, Africell a enfreint l’obligation de notifier et de demander l’autorisation préalable à l’APD pour le traitement des données personnelles de ses clients.

L’opérateur de réseau mobile a ainsi collecté diverses catégories de données à caractère personnel des personnes concernées. Or, en vertu de la loi sur la protection des données personnelles en Angola, outre le consentement des personnes concernées, l’entité qui traite des données personnelles doit informer l’APD avant d’effectuer des traitements de données à caractère personnel.

© Unsplash

Cependant, l’autorité a indiqué des circonstances juridiques qui ont atténué la responsabilité d’Africell dans cette violation. Tout d’abord, Africell a montré son intention manifeste et immédiate de se conformer à la loi, n’a pas d’antécédents

de violations des données et n'a pas tiré d'avantage économique de la situation qui s'est produite. En outre, Africell a rapidement coopéré avec l'APD, en fournissant les informations requises..

Bien que l'amende infligée à Africell soit inférieure au montant maximum de 418 000 euros, l'affaire souligne l'importance de respecter la loi sur la protection des données personnelles. Dans son communiqué de presse, l'APD a précisé que les entreprises qui collectent et traitent des données personnelles devaient obtenir le consentement des personnes concernées et respecter les obligations de notification et d'autorisation préalable à l'APD.

Convictions philosophiques ou politiques	❑ Oui	❑ Non
Appartenance à un parti ou à un syndicat	❑ Oui	❑ Non
Convictions religieuses	❑ Oui	❑ Non
Vie privée	❑ Oui	❑ Non
Origine raciale ou ethnique	❑ Oui	❑ Non
Santé et vie sexuelle	❑ Oui	❑ Non
Données génétiques	❑ Oui	❑ Non
Soupçons d'activités illégales	❑ Oui	❑ Non
Condamnations pénales	❑ Oui	❑ Non
Décisions imposant des mesures de sécurité	❑ Oui	❑ Non
Amendes, sanctions supplémentaires	❑ Oui	❑ Non
Amendes pour délits et contraventions	❑ Oui	❑ Non

Description des catégories de données personnelles contenues dans le formulaire de notification de traitement de l'APD

Afrique du Sud : l'autorité de protection des données publie un avis d'exécution contre le Ministère de la Justice

© Unsplash

L'autorité sud-africaine de protection des données (Information Regulator) a émis un avis d'exécution à l'égard du ministère de la Justice et du Développement constitutionnel (DoJ&CD), suite à la constatation de la violation de divers articles de la loi sur la protection des renseignements personnels (POPIA). En effet, en septembre 2021, le DoJ&CD a subi une compromission de la sécurité de ses systèmes informatiques. Cela a conduit à l'indisponibilité des systèmes du ministère pour ses employés et a par la suite affecté les services publics.

L'autorité a procédé à une évaluation de sa propre initiative après que le ministère a subi cette violation de données. Au cours de cette évaluation, l'autorité a constaté que le DoJ&CD n'avait pas mis en place les mesures techniques adéquates pour surveiller et détecter l'exfiltration non autorisée de données de son environnement, ce qui a entrainé la perte d'environ 1204 fichiers.

Cela s'est produit à la suite du non-renouvellement par le DoJ&CD de la licence SIEM (Security Incident and Event Monitoring), qui lui aurait permis de surveiller les activités inhabituelles sur son réseau et de conserver une sauvegarde des fichiers journaux. Ce non-renouvellement de la licence a entraîné l'indisponibilité des informations critiques contenues dans les fichiers journaux. La licence SIEM a, elle, expiré en 2020.

© Unsplash

De plus, le DoJ&CD n'a pas non plus renouvelé la licence du système de détection d'intrusion, qui avait également expiré en 2020. Si cette licence avait été renouvelée, le département aurait reçu des alertes d'activités suspectes de personnes non autorisées accédant au réseau. La licence Trend Antivirus n'a, elle non plus pas été renouvelée en 2020 lorsqu'elle a expiré. Le non-renouvellement de cette licence a entraîné la non-mise à jour de la définition de virus pour les menaces de logiciels malveillants connus. L'autorité a également constaté que le DoJ&CD n'avait pas pris de mesures nécessaires pour identifier les risques internes et externes raisonnablement prévisibles pour la protection des données personnelles en sa possession ou sous son contrôle. Enfin, le DoJ&CD n'avait pas non plus établi ni maintenu de garanties appropriées contre les risques identifiés.

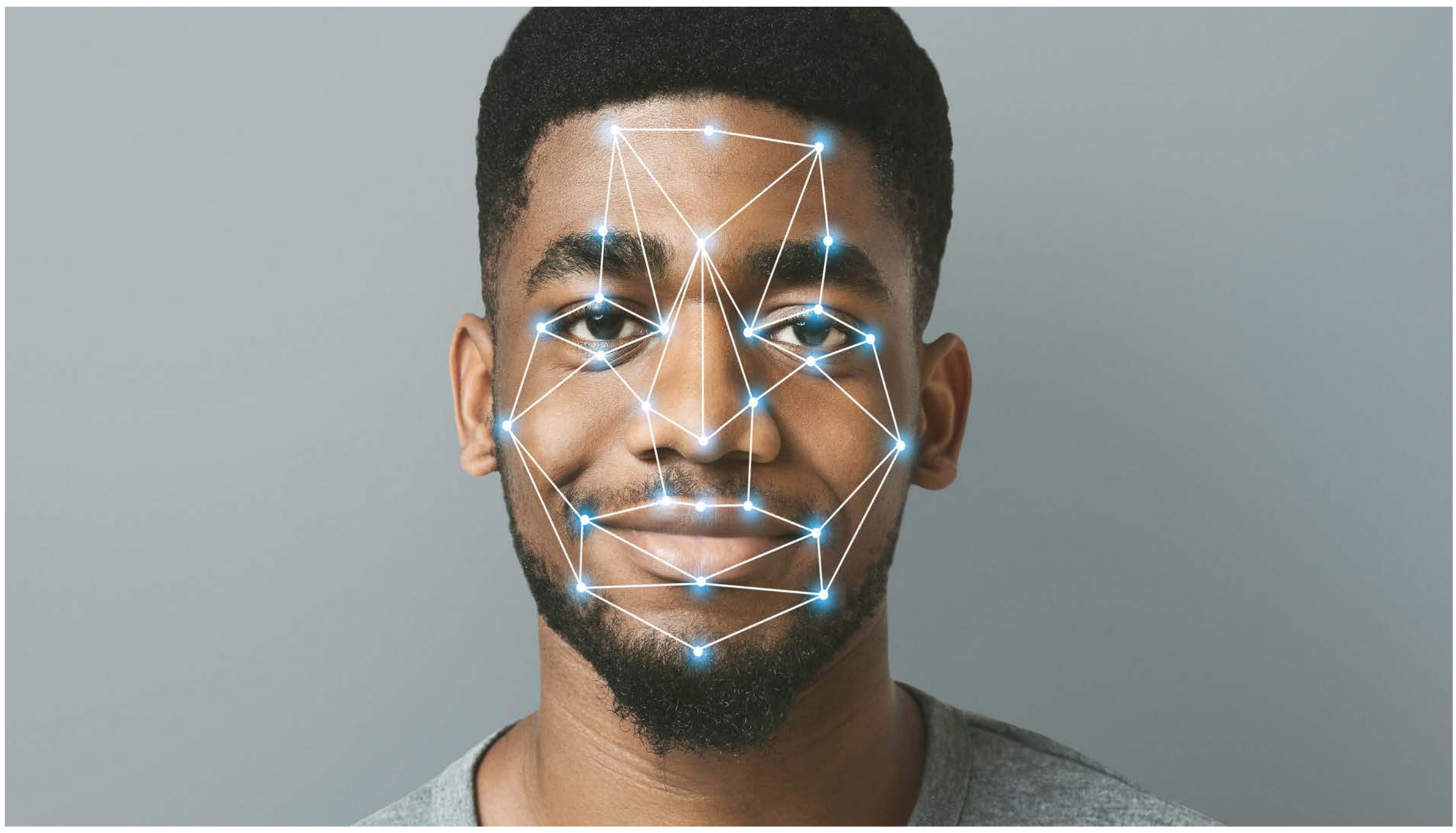
Par ailleurs, le ministère a omis d'établir et de maintenir des mesures de protection appropriées contre les risques identifiés et de vérifier et mettre à jour régulièrement les mesures de sécurité contre les menaces de logiciels malveillants. Après avoir constaté que le DoJ&CD avait enfreint les articles 19 et 22 du POPIA, Information Regulator lui a envoyé un avis d'exécution dans lequel il ordonnait au ministère de prendre un certain nombre de mesures. Parmi celles-ci, il est indiqué que le ministère devra fournir une preuve à l'autorité dans les 31 jours suivant la réception de l'avis que la licence Trend Anti-Virus, la licence SIEM et la licence du système de détection d'intrusion ont été renouvelées. Il devra également engager une procédure disciplinaire à l'encontre du ou des fonctionnaires qui n'ont pas renouvelé les autorisations nécessaires pour protéger le service contre les atteintes à la sécurité. Si le DoJ&CD ne respecte pas l'avis d'exécution dans le délai imparti, il sera coupable d'une infraction, en vertu de laquelle l'autorité pourra imposer une amende administrative, ou, sur condamnation, l'emprisonnement des fonctionnaires responsables.

Avec l'augmentation des compromissions en matière de sécurité, l'autorité de protection des données met désormais l'accent sur la gestion des risques.

© Unsplash

Elle invite les responsables de traitement à améliorer leurs systèmes de sécurité de l'information, afin de s'assurer qu'il existe des garanties adéquates pour protéger les données personnelles des personnes concernées, en leur possession ou sous leur contrôle.

Sénégal : Brioche Dorée se voit refuser sa demande d'autorisation de système biométrique par reconnaissance faciale



© iStock

Au cours du premier trimestre de l'année 2023, la Commission de protection des Données Personnelles du Sénégal (CDP) a décidé de refuser à la Brioche Dorée, une entreprise de restauration rapide, une demande d'autorisation d'exploitation d'un système biométrique par reconnaissance faciale, à des fins de contrôle du temps de présence, des entrées et des sorties de ses salariés.

La CDP a estimé, en effet, qu'un tel système, qui collecte des données faciales, était excessif au regard des finalités de sécurisation des locaux, de contrôle du temps de présence et de maîtrise des entrées et sorties des employés.

L'autorité de protection des données a donc demandé à la Brioche Dorée de mettre en place un système moins intrusif de contrôle du temps de présence, des entrées et sorties des salariés, notamment en ayant recours au système de pointage digital.

Algérie : l'autorité de protection des données (ANPDP) lance son site web

L'Autorité Nationale de Protection des Données à Caractère Personnel (ANPDP) a lancé officiellement, le 30 janvier 2023 son internet.

A l'occasion de l'annonce du lancement officiel du site , le président de l'ANPDP, Lotfi Boudjemaa, a précisé qu'il visait, dans sa première étape allant de janvier à août 2023, à sensibiliser et informer les personnes concernées et les responsables du traitement des données de leurs droits et obligations. Ils pourront pour cela prendre connaissance du contenu de la loi relative à la protection des personnes physiques en matière de données à caractère personnel, qui définit les droits et sanctions prévues en cas d'atteinte à ces informations.

Dans sa deuxième étape, l'autorité a fait savoir qu'elle inclurait tous les formulaires relatifs au traitement, et ce conformément aux dispositions de cette loi.

Formulaires de déclaration des traitements
Formulaire de désignation du responsable de traitement ou de son remplaçant habilité
Formulaire de demande d'autorisation (déclaration préalable) pour la réalisation des nouveaux traitements de données à personnel à caractère personnel
Formulaire de demande d'autorisation de transfert des données personnelles à l'étranger
Formulaire de demande d'autorisation de l'interconnexion des fichiers
Formulaire de demande d'autorisation de traitement des données sensibles
Formulaire de demande d'avis
Formulaires des réclamations, des recours et des plaintes

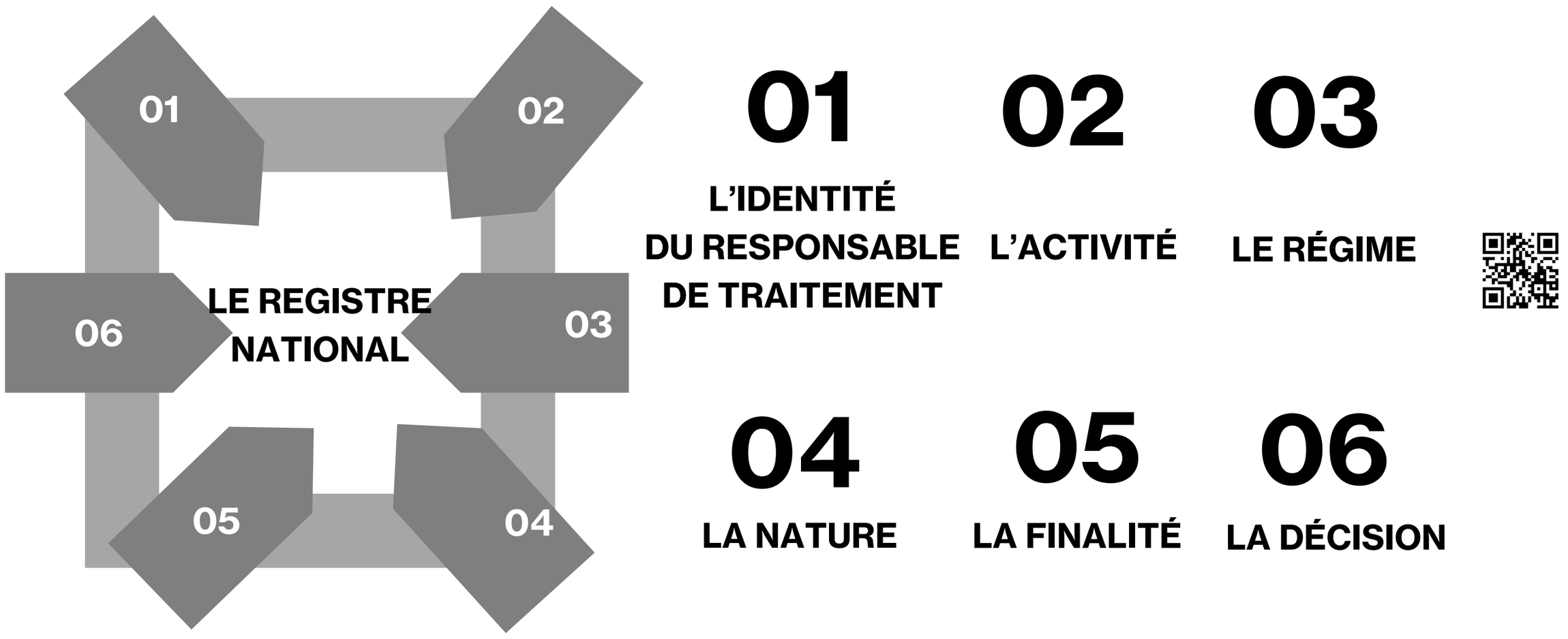
Liste des formulaires qui seront disponibles à compter du mois d'août 2023

Le président a en outre précisé : "la mise en service de ce site web permettra d'établir un contact direct entre les personnes et les organismes publics et privés ayant trait au travail de l'autorité".

Maroc : la CNDP publie son registre national de la protection des données

© Unsplash

La Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) à mis à la disposition du public le registre national de la protection des données à caractère personnel. Les articles 45 à 50 de la loi n°09-08 confèrent à la CNDP la tenue de ce registre.



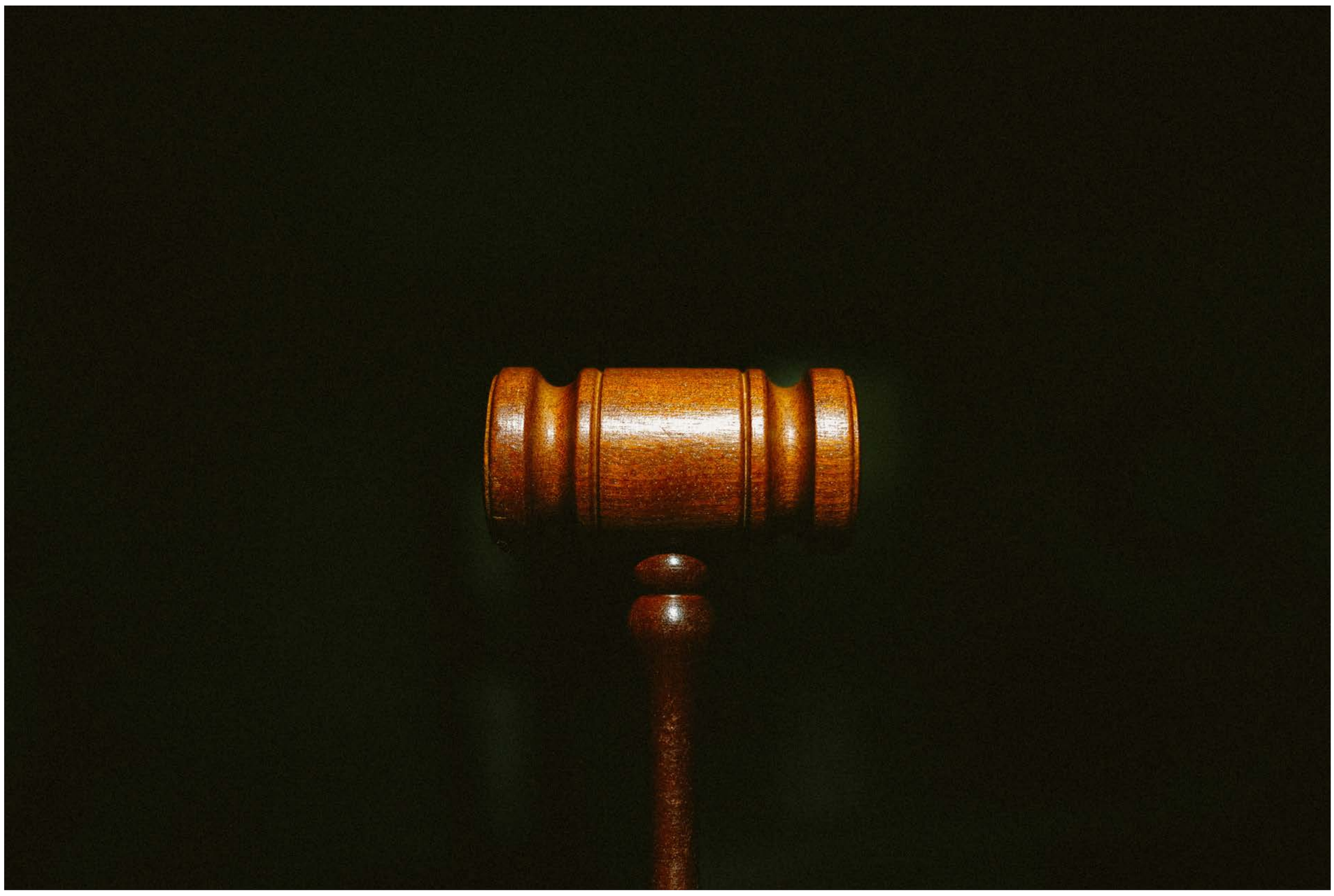
Principaux champs contenus dans le registre national

La CNDP a également précisé que les responsables de traitement pouvaient demander des corrections, des modifications ou des compléments, à considérer au sein de ce registre national.

Bénin : mise en œuvre des missions de contrôle

Des Officiers de police judiciaire et des agents assermentés du service contrôle et contentieux de l'Autorité de Protection des Données Personnelles (APDP) ont tenu une série de rencontres d'opérationnalisation des contrôles de conformité des traitements et de visites sur site tout au long du mois de Mars 2023.

Ces rencontres font suite aux dispositions du code du numérique qui confèrent à l'APDP le pouvoir d'effectuer des enquêtes, des vérifications et des contrôles des traitements de données à caractère personnel sur le territoire de la République du Bénin.



© Unsplash

Les membres de l'autorité ainsi que les agents de ses services assurent le contrôle de la mise en œuvre du traitement. À cet effet, ils ont accès, de six heures à vingt-et-une heures, dans l'exercice de leur mission, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel.

Les Ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et, plus généralement, les détenteurs et utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent, en principe, s'opposer à l'action de l'Autorité.

Cette formation conjointe est un prélude aux missions de contrôle qu'elle initiera sans doute désormais sur toute l'étendue du territoire national.

Il est important de souligner que l'APDP dispose de pouvoirs étendus pour s'assurer que les traitements de données à caractère personnel sont conformes à la loi en vigueur. Les responsables de traitement qui ne respectent pas les règles pourront se voir infliger des sanctions administratives et

© Unsplash

Cette initiative de l'APDP devrait contribuer à améliorer la protection des données personnelles au Bénin en garantissant le respect des droits fondamentaux des citoyens en matière de vie privée et de protection des données personnelles.

Côte d'Ivoire : l'autorité de protection des données prononce 2 mises en demeure à la suite du plan de contrôle

Dans le cadre de ses missions, l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI), a porté à la connaissance des entreprises, des organismes publics, et des particuliers que des contrôles en matière de protection des données personnelles et de vie privée seraient effectués sur toute l'étendue du territoire national, du 12 juillet 2022 au 30 novembre 2022.

© iStock

A l'issue de ces contrôles, deux organismes ont été mis en demeure. La première mise en demeure concerne un hôtel. Le tableau suivant résume les principaux manquements.

L'absence d'autorisation de traitement de données ;
L'absence de mise en conformité à la loi relative à la Protection des données à caractère personnel ;
L'absence de garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relative aux traitements à effectuer par les sous-traitants ;
Le non-respect des principes liés à la protection des données à caractère personnel par l'Hôtel et ses sous-traitants ;
Le non-respect des principes de la légitimité, de la proportionnalité, de la durée limitée de la conservation des données, droits des personnes concernées, de la transparence ;
Le non-respect de l'information des personnes concernées et de la transparence ;
La méconnaissance du personnel de l'Hôtel en matière de protection des données personnelles ;

L’absence d’autorisation pour le dispositif de vidéosurveillance ;
L’absence d’autorisation pour le dispositif de biométrique ;
L’inexistence d’affiche ou de pictogramme pour la vidéosurveillance ;
L’absence de procédure relative aux droits des personnes concernées ;
L’absence de preuve garantissant Is respect de la Protection des données personnel traitées par les logiciels utilisés au sein de l’Hôtel ;
Les transferts de données à caractère personnel non autorisés vers le SENEGAL et la TUNISIE ;
La non-désignation du correspondant à la Protection des données à caractère personnel.

La deuxième mise en demeure concerne un cabinet spécialisé dans le recrutement. Les principaux manquements sont cités dans le tableau suivant.

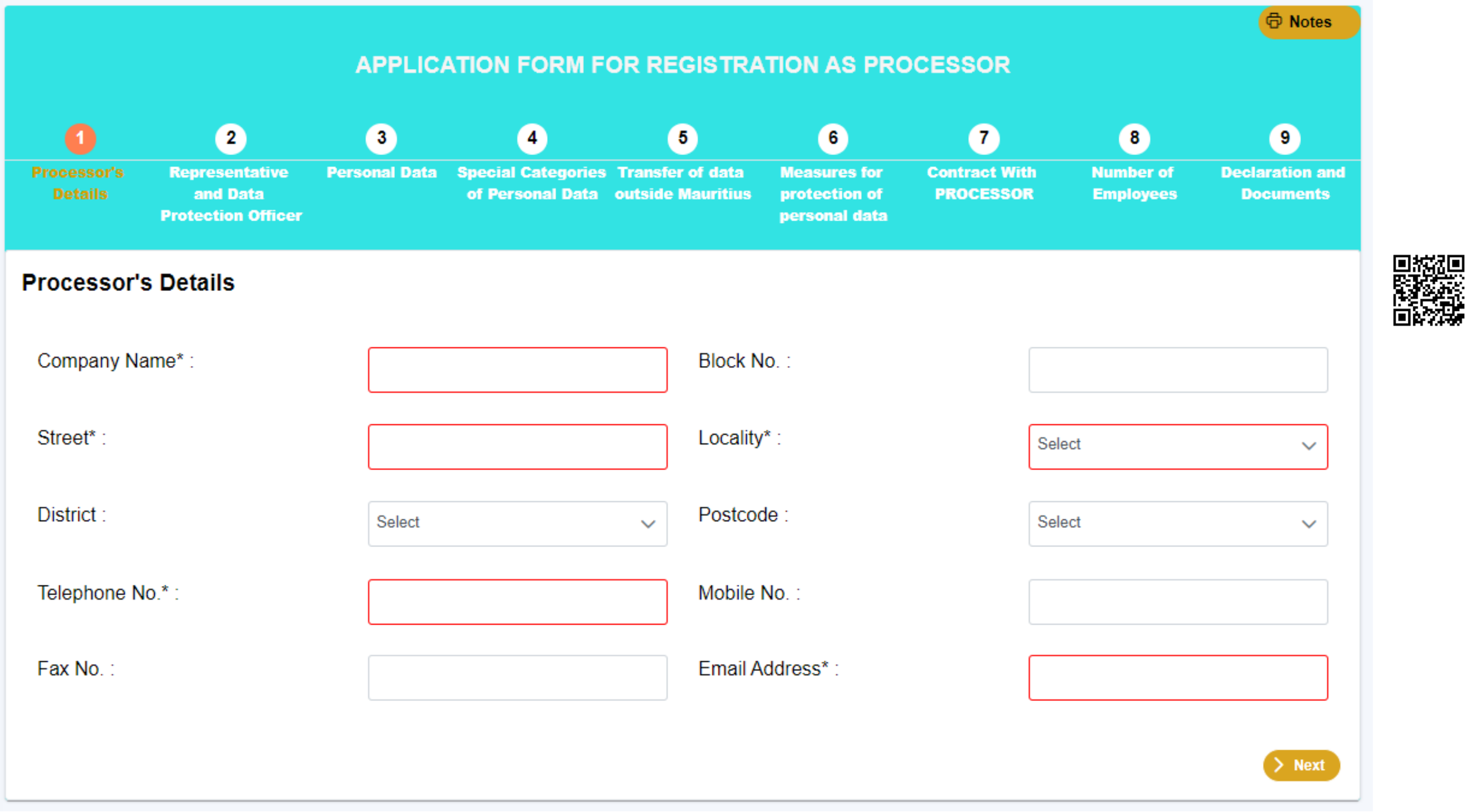
L’absence d’autorisation de traitement de donnée ;
L’absence de mise en conformité à la loi relative à la protection des données à caractère personnel ;
L'absence de garanties suffisantes au regard des mesures de sécurité techniques et d’organisation relatives aux traitements à effectuer par les sous-traitants ;
Le non-respect des principes liés à légitimité, de la durée limitée de la conservation des données, droits des personnes concernées, de la transparence ;
Le non-respect de l’information des personnes concernées et de la transparence ;
L’absence de procédure relative aux droits des personnes concernées ;
Les transferts de données non autorisés vers la France ;
La non-désignation du correspondant à la protection des données à caractère personnel ;
L’insuffisance des mesures de sécurité et de confidentialité des données.

L’ARTCI a précisé dans ses décisions, l’obligation pour ces entreprises de se mettre en conformité avec la loi dans les soixante jours à compter de la réception des avertissements.

© Unsplash

Île Maurice : l'autorité de protection des données lance son portail d'enregistrement en ligne e-DPO

Le portail du DPO (Data Protection Office), l'autorité mauricienne de protection des données a été lancé en décembre 2022. C'est une plateforme en ligne où les entreprises, les organisations et les particuliers peuvent s'inscrire en tant que responsable de traitement ou sous-traitant et soumettre des formulaires. Il s'agit d'une plateforme unique où l'utilisateur peut soumettre ou interroger l'état d'une demande, télécharger des certificats ou payer des frais. C'est le guichet unique pour interagir avec l'autorité de protection des données.



Exemple d'interface web de la plateforme e-DPO

Cette interface permet de renseigner des informations telles que: les coordonnées du responsable de traitement et du délégué à la protection des données, les catégories des données traitées , les éventuels transfert de données hors de l'île Maurice et les mesures de sécurité. L'autorité de protection des données a précisé sur son site qu'il fallait désormais utiliser la plateforme e-DPO pour communiquer avec elle.