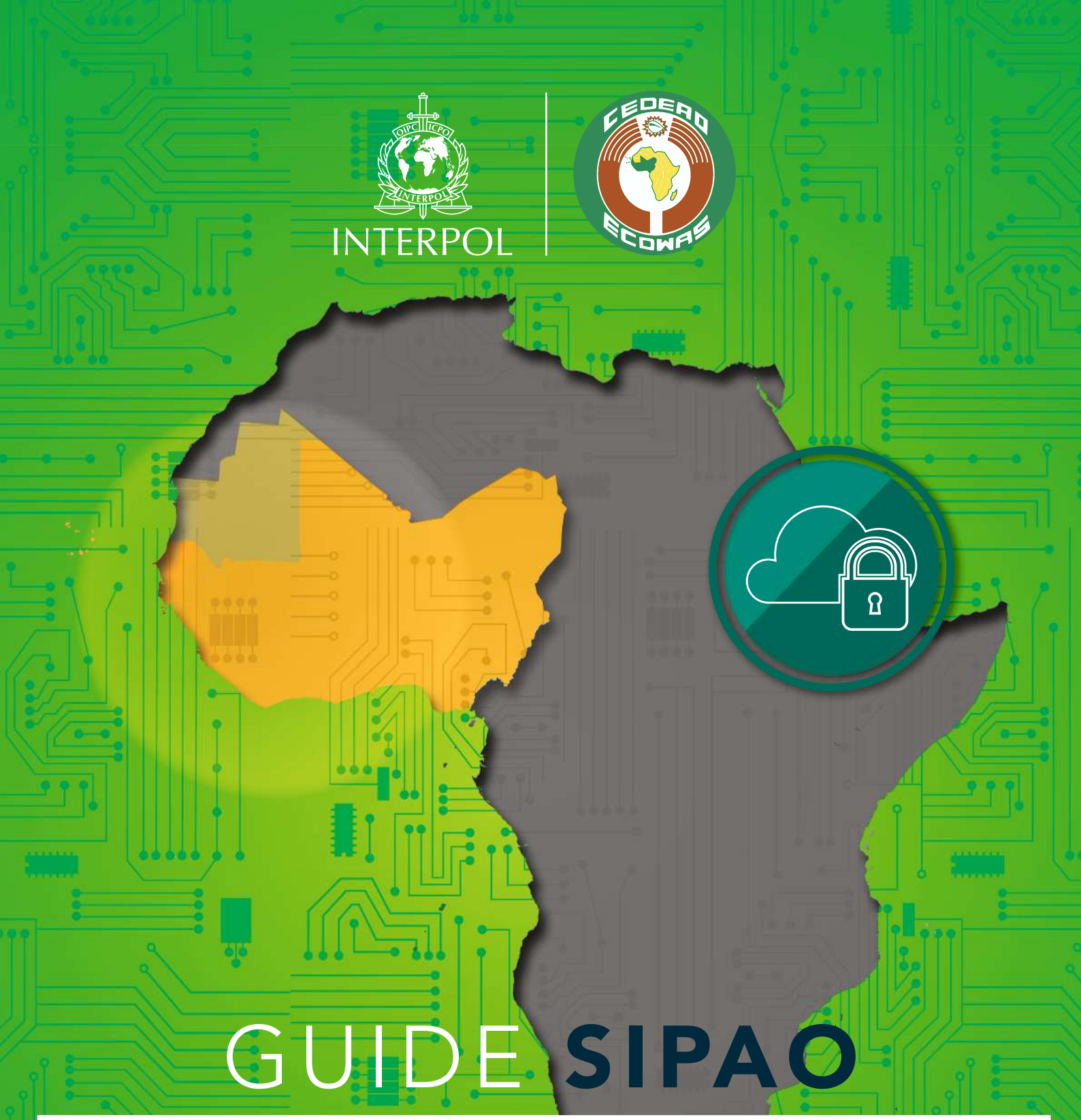
INTERPOL



GUIDE SIPAO

LES BONNES PRATIQUES EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

JUIN 2020

Ce projet est financé par l'Union Européenne

Le Guide de bonnes pratiques en matière de protection des données à caractère personnel du Système d'information policière pour l'Afrique de l'Ouest a été élaboré par l'Equipe du Programme SIPAO sous les auspices du Bureau des Affaires Juridiques d'INTERPOL et avec les contributions précieuses de Madame Teki Akuetteh et du Dr Mouhamadou Lo, tous deux experts en matière de protection des données.

Ce projet est financé par l'Union Européenne

GÉNÉRAL FRANCIS A. BEHANZIN
Commissaire aux Affaires Politiques, Paix et Sécurité de la CEDEAO

PRÉFACE

En voulant aborder une étape importante (partage des renseignements criminels) pour une meilleure gestion de la lutte contre le crime organisé en général et le terrorisme en particulier en Afrique de l'Ouest, il convient de tirer un chapeau à l'OIPC-INTERPOL qui, avec son expérience presque séculaire (1923-2020) de bientôt 100 ans dans le domaine d'investigations policières, apporte à la CEDEAO à travers l'Union Européenne qui le finance, le « Système d'Information Policière pour l'Afrique de l'Ouest » (SIPAO) pour les 15 Etats membres de la CEDEAO ainsi que la Mauritanie. En effet, développé à l'origine pour faciliter la constatation d'infractions à la loi pénale, le rassemblement de preuves relatives aux infractions et la recherche de leurs auteurs et complices éventuels, en vue de lutter contre la criminalité transnationale et le terrorisme, la mise en œuvre du Programme SIPAO engendre par ricochet un traitement de données à caractère personnel et prévoit également que les données concernant les témoins et victimes puissent être enregistrées si les nécessités de l'enquête l'exigent. Dans la progression de cet important projet de la CEDEAO, les agences chargées de l'application de la loi (Police, Gendarmerie, Douanes, Immigration, Eaux et Forêts et Assimilés) seront amenées à se partager des informations sensibles à la fois sur les personnes et les biens dans le but ultime de sécuriser les personnes et les biens dans l'espace CEDEAO, dans le Continent Africain, en Europe et dans le Monde entier. Il s'agira pour ces services précités de se partager des données à caractère personnel, c'est à dire toutes informations relatives à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Ces données sont protégées en Afrique de l'Ouest par l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO, adopté le 16 février 2010 pour prémunir les citoyens de la Communauté de tous abus dans la collecte et le traitement de ces « données dites personnelles ». L'Acte additionnel a donc établi les principes fondamentaux applicables au traitement des données à caractère personnel et enjoint aux Etats membres de la CEDEAO d'adopter des lois relatives à la protection de ce type de données et de mettre en place des autorités de protection adéquate, donc chargées de faire appliquer le droit de la protection des données à caractère personnel.

POURQUOI PROTÉGER LES DONNÉES PERSONNELLES ?

Protéger les données à caractère personnel revient à protéger l'intimité, la dignité et les autres droits fondamentaux de la personne comme, le droit à la vie privée, le droit à l'image, le droit à l'honneur, etc.

C'est dans ce contexte, et dans l'objectif d'assister les services d'application de la loi dans leur traitement des données à caractère personnel dans le SIPAO conformément à l'Acte additionnel, aux autres lois et règlementations applicables au sein des pays concernés ainsi qu'aux normes internationales de protection des données, que le présent Guide de bonnes pratiques en matière de protection des données à caractère personnel a été développé.

Ce Guide, élaboré par le Programme SIPAO et approuvé par les représentants des pays participant à ce Programme lors des rencontres d'harmonisations juridiques du Comité d'Experts de la CEDEAO qui se sont tenues à Abidjan des 22 au 24 octobre 2019, s'appuie sur les bonnes pratiques nationales et internationales conformément à l'Acte additionnel et aux législations en vigueur dans les pays participants au Programme. Ce Guide des bonnes pratiques, sans être contraignant, a vocation à être un outil d'orientation visant à faciliter la compréhension des normes en vigueur ainsi que des lignes directrices régissant la collecte, le traitement, le partage, l'utilisation et la conservation des données à caractère personnel dans le cadre du Programme SIPAO.

Une mise en œuvre adéquate du présent Guide par les services d'application de la loi permettra aux pays participant au Programme d'adopter les meilleures pratiques qui faciliteront le partage des informations et optimiseront l'utilisation du SIPAO tout en assurant l'équilibre indispensable entre l'efficacité du système répressif et le respect des droits et libertés fondamentaux reconnus à tout individu.

J'engage les pays participant au Programme SIPAO à tirer le plus grand profit professionnel de ce Guide pour optimiser leur capacité à lutter contre la criminalité transnationale et le terrorisme grâce à un partage d'informations de qualité.

Général Francis A. BEHANZIN
Commissaire aux Affaires Politiques, Paix et Sécurité

TABLE DES MATIÈRES

INTRODUCTION

NATURE DU GUIDE DES BONNES PRATIQUES DU SIPAO EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

L'objectif du Guide des bonnes pratiques (« GBP ») en matière de protection des données à caractère personnel du Système d'information policière pour l'Afrique de l'Ouest (« SIPAO » ou « le Système ») est d'aider les services chargés de l'application de la loi à traiter les données dans le SIPAO dans le respect de l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO (« l'Acte additionnel »), des autres lois et réglementations applicables au sein des pays concernés, ainsi que des normes et bonnes pratiques internationales en matière de traitement des données à caractère personnel.

Le GBP du SIPAO s'adresse à l'ensemble des services chargés de l'application de la loi et des entités qui traitent des données à caractère personnel en utilisant le Système. Il fournit des orientations sur la protection des données aux fins du traitement des données à caractère personnel dans ledit Système. Il vise à faciliter la compréhension de la législation en vigueur ainsi que des lignes directrices en matière d'application de la loi régissant le traitement des données par les services chargés de l'application de la loi des pays participant au SIPAO.

Le GBP du SIPAO n'exonère nullement les États membres de la CEDEAO de leurs obligations au titre de l'Acte additionnel, notamment celles requérant l'adoption d'une législation nationale relative à la protection des données et la mise en place d'une autorité de protection des données.

Le GBP du SIPAO est un outil d'orientation en matière de protection des données élaboré spécifiquement pour les pays participant au SIPAO afin de garantir l'adoption de bonnes pratiques lors de la collecte, du traitement, du partage et de l'utilisation des données à caractère personnel dans le Système. Il s'appuie sur les bonnes pratiques nationales et internationales, conformément à l'Acte additionnel de la CEDEAO et à la législation des pays participant au SIPAO qui ont adopté des lois en matière de protection des données. Il définit les principes, dérogations et droits fondamentaux applicables en matière de protection des données, tout en s'attachant aux structures de gouvernance et de conformité qui en faciliteront la mise en œuvre.

UTILITÉ DU GBP DU SIPAO

Le SIPAO est un système électronique d'information policière mis en œuvre au niveau national, régional et international. Son objectif global est de renforcer la capacité des

services chargés de l'application de la loi d'Afrique de l'Ouest à lutter contre la criminalité transnationale et le terrorisme grâce à l'amélioration de la gestion et du partage d'informations. Le Système contiendra des informations en matière d'application de la loi, notamment sur :

a. des personnes (comme les suspects, les témoins et les victimes) ;
b. des moyens de transport (comme les voitures) ;
c. des documents (comme les passeports, les permis de conduire, les cartes nationales d'identité, etc.) ;
d. des armes ;
e. des lieux ;
f. des événements ;
g. des éléments génériques (par exemple, des éléments trouvés sur une scène d'infraction qui ne correspondent pas aux catégories définies).

Certaines de ces informations répondent à la définition de « données à caractère personnel », puisqu'elles permettent d'identifier, directement ou indirectement, une personne physique.

Au niveau régional, les Hautes Parties Contractantes de la CEDEAO, conscientes du préjudice que le traitement des données à caractère personnel peut causer sur les droits et libertés fondamentaux des personnes concernées, ont adopté l'Acte additionnel le 16 février 2010. Cet Acte établit les principes fondamentaux applicables au traitement des données à caractère personnel dans l'espace de la CEDEAO et requiert de ses États membres qu'ils adoptent des lois en matière de protection des données et instaurent une autorité de protection des données. La mise en œuvre de ces exigences essentielles est variable en fonction des pays participant au SIPAO.

Le présent GBP est une réponse à la demande formulée au cours du séminaire juridique sur le SIPAO, organisé les 19 et 20 mars 2019 à l'initiative de la Commission de la CEDEAO, d'INTERPOL et de l'Union européenne, et qui a réuni les points focaux et les experts juridiques du SIPAO des 16 pays participant au Système. Face aux inquiétudes relatives à l'absence d'une législation adéquate et d'une autorité de protection des données dans certains pays participant au SIPAO, il a été proposé d'élaborer un projet de guide des « bonnes pratiques » en matière de traitement des données à caractère personnel dans le SIPAO et de le soumettre pour examen aux points focaux et aux experts juridiques du SIPAO au cours d'un atelier juridique dédié. Le projet de GBP a été présenté au cours d'un séminaire juridique de suivi, également organisé à l'initiative de la Commission de la CEDEAO, d'INTERPOL et de l'Union européenne, qui s'est tenu à Abidjan du 22 au 24 octobre 2019 et a été approuvé par les participants.

PRÉSENTATION DU GBP DU SIPAO

Le présent Guide se compose de douze chapitres.
Le premier chapitre présente les termes et expressions utilisés dans le Guide. Il définit en particulier les termes et expressions afférents aux principales entités responsables de la protection des données à caractère personnel au titre du Guide (Ch. 1, para. 1 et 2), les destinataires des données à caractère personnel (Ch. 1, para. 8), les personnes dont les données à caractère personnel sont traitées (Ch. 1, para. 4) et le type d'informations constituant des données à caractère personnel (Ch. 1, para. 7).

Le deuxième chapitre présente les principes généraux de la protection des données à caractère personnel et les finalités légitimes en matière d'application de la loi qui en justifient le traitement. Les principes de la protection des données à caractère personnel fournissent un cadre général aux services chargés de l'application de la loi pour leur permettre de comprendre les différentes exigences applicables au traitement des données à caractère personnel dans le SIPAO. Les principes de la protection incluent : a) consentement et légitimité ; b) licéité et loyauté ; c) finalité, pertinence et conservation ; d) exactitude ; e) transparence ; f) confidentialité et sécurité ; g) choix du sous-traitant. Les services chargés de l'application de la loi ne doivent traiter de données dans le SIPAO qu'au titre des finalités légitimes en matière d'application de la loi, notamment : la prévention, les enquêtes, la détection et les poursuites dans le cadre d'infractions ; l'exécution des sanctions ; le maintien de l'ordre public ; la protection contre les menaces à la sécurité publique et la prévention de ces dernières ; ou toute obligation ou responsabilité légale qui leur incombent.

Le troisième chapitre aborde le rôle des autorités de protection des données, l'importance de la formation à la protection des données et l'importance d'engager les parties prenantes clés pour qu'elles participent à la mise en œuvre du cadre de protection des données. En premier lieu, tous les pays participant au SIPAO doivent mettre en place une autorité de protection des données indépendante, responsable de la supervision de toutes les opérations de traitement des données. En deuxième lieu, les services chargés de l'application de la loi doivent désigner un officier délégué à la protection des données chargé de : a) les conseiller quant aux obligations légales qui leur incombent ; b) contrôler la conformité ; c) fournir des conseils sur les analyses d'impact relatives à la protection des données ; d) assurer la liaison avec les autorités de protection des données ; e) mettre en place des programmes de formation continue adaptés destinés aux utilisateurs du SIPAO. En dernier lieu, les services chargés de l'application de la loi doivent intégrer la protection des données à leur structure de gouvernance en impliquant les parties prenantes clés dans le cadre de protection des données du SIPAO.

Le quatrième chapitre présente les bonnes pratiques en matière de collecte et de partage des données à caractère personnel. De manière générale, la collecte des données à caractère personnel doit être limitée à ce qui est nécessaire et proportionné à la finalité pour laquelle elles sont collectées.

Le cinquième chapitre aborde la question de la qualité des données et les mesures que les services chargés de l'application de la loi doivent mettre en œuvre pour préserver la confidentialité et la sécurité des données à caractère personnel. De manière générale, les services chargés de l'application de la loi ne doivent pas partager de données à caractère personnel inexactes, incomplètes ou obsolètes. S'ils partagent des données à caractère personnel inexactes, ils doivent en avertir sans tarder le destinataire et prendre les mesures nécessaires pour les rectifier, les effacer ou en restreindre le traitement. De plus, ils doivent prendre des mesures permettant de sécuriser le SIPAO.

Le sixième chapitre énonce les mesures à déployer pour répondre de manière adaptée à une violation de données. Les services chargés de l'application de la loi doivent répertorier et signaler sans délai les violations de données à l'autorité de protection des données concernée, de préférence dans les 72 heures à compter de la violation initiale. De plus, ils doivent avertir sans délai les personnes concernées de toute violation de données si celleci est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Le septième chapitre présente les bonnes pratiques en ce qui concerne le traitement des registres et la conservation des données. Les services chargés de l'application de la loi doivent conserver des registres de toutes les activités de traitement de données. De plus, ils doivent conserver des journaux sur les opérations de traitement des données suivantes : a) collecte ; b) modification ; c) accès/consultation ; d) communication, dont les transferts ; e) interconnexion ; f) effacement. En outre, les données ne doivent être conservées que pour une période adéquate.

Le huitième chapitre explique que les données sensibles (« données à caractère personnel qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'orientation sexuelle, ainsi que les données génétiques, ou plus généralement les données sur l'état de santé d'une personne physique » [Ch. 8.1, para. 1]) ne doivent être traitées dans le SIPAO qu'en cas de nécessité absolue.

Le neuvième chapitre présente les droits des personnes concernées, à savoir les droits d'accès, de rectification ou d'effacement. Le droit d'accès permet à une personne d'accéder, directement ou indirectement, aux données qui la concernent et qui sont

traitées dans le SIPAO, tandis que le droit de rectification ou d'effacement lui permet de demander aux services chargés de l'application de la loi de rectifier ou d'effacer des données à caractère personnel inexactes la concernant qui sont enregistrées dans le Système.

Le dixième chapitre aborde les analyses d'impact relatives à la protection des données, un processus qui peut aider les services chargés de l'application de la loi à évaluer et consigner les risques encourus lors du traitement des données à caractère personnel dans le SIPAO. Une analyse d'impact relative à la protection des données exécutée de manière adéquate prouvera que les services chargés de l'application de la loi ont tenu compte des risques afférents au traitement des données prévu.

Le onzième chapitre recense les situations où les données peuvent ne pas être traitées conformément au présent Guide.

Le douzième chapitre fait la synthèse de l'objectif global du présent Guide, qui est de permettre aux pays participant au SIPAO d'adopter des pratiques de traitement des données légales qui facilitent le partage des informations et optimisent l'utilisation du SIPAO.

CHAPITRE I

TERMES ET EXPRESSIONS

Aux fins du présent Guide :

1. « Responsable du traitement » désigne toute personne physique ou morale, publique ou privée, 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 finalités1.
2. « Soustraitant » désigne toute personne physique ou morale, publique ou privée, ou tout autre organisme ou association qui traite des données pour le compte du responsable du traitement2.
3. « Autorité de protection des données » désigne l'organisme indépendant chargé d'assurer la protection des données mis en place par le pays participant au SIPAO conformément à l'article 14 de l'Acte additionnel et/ou de la législation locale du pays participant.
4. « Personne concernée » désigne toute personne physique dont les données à caractère personnel font l'objet d'un traitement3.
5. « Violation de données à caractère personnel » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées, ou l'accès non autorisé auxdites données4.
6. « Traitement des données à caractère personnel » désigne toute opération ou série d'opérations effectuée à l'aide de procédés automatisés ou non, et appliquée à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, 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 des données à caractère personnel5.
7. « Données à caractère personnel » désigne toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par

1 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

2 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

3 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

4 Règlement général sur la protection des données, Article 4.12.

5 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique[6].

8. « Destinataire » désigne toute personne physique ou morale habilitée à recevoir 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[7].
9. « Données sensibles » désigne toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques et syndicales, à l'orientation sexuelle ou aux origines raciales, à la santé, aux mesures d'ordre social, aux poursuites et aux sanctions pénales ou administratives[8].
10. « Acte additionnel » désigne l'Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.
11. « Pays participant au SIPAO » fait référence aux pays suivants : République du Bénin, Burkina Faso, République du Cap Vert, République de Côte d'Ivoire, République de Gambie, République du Ghana, République de Guinée, République de GuinéeBissau, République du Libéria, République du Mali, République islamique de Mauritanie, République du Niger, République fédérale du Nigéria, République du Sénégal, République de Sierra Leone, République du Tchad et République togolaise.
12. « SIPAO » (ou le « Système ») désigne le Système d'information policière pour l'Afrique de l'Ouest, un système d'information policière électronique mis en œuvre au niveau national, régional et international.

---

6 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

7 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

8 Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du 16 février 2010, Article 1.

CHAPITRE II

PRINCIPES RÉGISSANT LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET FINALITÉ DU TRAITEMENT

2.1 PRINCIPES APPLICABLES

Lors du traitement des données à caractère personnel dans le Système, les principes suivants, énoncés au Chapitre V de l'Acte additionnel, doivent guider les services chargés de l'application de la loi :

1. Principe de consentement et de légitimité : les services chargés de l'application de la loi doivent traiter les données à caractère personnel pour des motifs légitimes, notamment en s'assurant que le traitement est nécessaire en vue de :
   - **a.** respecter une obligation légale qui leur incombe ;
   - **b.** remplir une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont ils sont investis.

   Les traitements ayant pour but l'application de la loi comme indiqué au paragraphe 2.2 ci-dessous sont exclus de l'obligation de requérir le consentement de la personne concernée.

2. Principes de licéité et de loyauté : les services chargés de l'application de la loi doivent traiter les données à caractère personnel de manière licite, loyale et non frauduleuse. Tout traitement doit être autorisé par la loi et respecter les droits fondamentaux des personnes concernées, conformément aux obligations applicables en matière de droits de l'homme. Le principal objectif est de protéger les intérêts des personnes physiques dont les données à caractère personnel sont traitées. Ce principe s'applique à toutes les actions entreprises sur ou avec les données à caractère personnel dans le Système. Il est important de souligner que le traitement des données à caractère personnel n'est pas nécessairement déloyal, déraisonnable ou illicite, même s'il cause un préjudice aux personnes concernées. Il est alors nécessaire de déterminer si le préjudice est justifiable au regard de la loi dans le cadre de la détection, de la prévention et de l'application de la loi. En pratique, cela signifie que les services chargés de l'application de la loi doivent :
   - **a.** avoir des motifs légitimes pour collecter, utiliser et traiter les données à caractère personnel dans le Système ;
   - **b.** s'abstenir d'utiliser les informations ou les données d'une manière qui causerait un préjudice injustifiable aux personnes concernées ;
   - **c.** faire preuve de transparence quant à l'utilisation prévue des données et

publier des avis relatifs à la protection des données ;

d. traiter les données à caractère personnel uniquement de la manière raisonnablement attendue dans le cadre du Système ;

e. s'assurer que les utilisateurs du Système ne commettent aucun acte illicite avec les données à caractère personnel.

3. Principe de finalité, de pertinence et de conservation : les services chargés de l'application de la loi doivent collecter des données à caractère personnel pour des finalités déterminées, explicites et légitimes, tout en veillant à ce que ces données ne soient traitées ultérieurement de manière incompatible avec ces finalités. Les données à caractère personnel doivent être adéquates et pertinentes au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement. Elles doivent être conservées pour une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées. Audelà de cette période, les données ne peuvent faire l'objet d'une conservation qu'en vue de leur traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

4. Principe d'exactitude : les services chargés de l'application de la loi doivent veiller à ce que les données à caractère personnel collectées soient exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

5. Principe de transparence : les services chargés de l'application de la loi sont tenus de communiquer sur le traitement des données à caractère personnel, sous réserve des dérogations applicables.

6. Principe de confidentialité et de sécurité : les services chargés de l'application de la loi doivent s'assurer que les données enregistrées dans le Système sont traitées de manière confidentielle et qu'elles sont protégées. Le niveau de confidentialité des données traitées dans le Système doit être déterminé en fonction des risques encourus par les personnes concernées et par les sources en cas de divulgation.

7. Principe de choix du soustraitant : les services chargés de l'application de la loi ont l'obligation, lorsque le traitement est effectué pour le compte d'un service chargé de l'application de la loi, de choisir un soustraitant présentant des garanties suffisantes. Il incombe au service chargé de l'application de la loi ainsi qu'au soustraitant de veiller au respect des principes applicables à la protection des données.Éviter toute collecte illégale de données à caractère personnel

CHAPITRE II

8. Respecter les droits fondamentaux des personnes concernées, notamment les droits de l'homme
9. Éviter tout traitement déloyal, déraisonnable ou illicite des données à caractère personnel
10. Veiller à ce que tout traitement ait une finalité déterminée, explicite et légitime
11. Fixer et gérer les délais de conservation des données à caractère personnel
12. Veiller à ce que les données à caractère personnel collectées soient exactes et, si nécessaire, mises à jour
13. Prendre des mesures pour effacer ou rectifier les données inexactes ou incomplètes
14. Être transparent quant à la gestion des données à caractère personnel
15. Sécuriser le Système et assurer la confidentialité des données à caractère personnel
16. Encadrer l'intervention des sous-traitants dans le Système

2.2 FINALITÉ DU TRAITEMENT DES DONNÉES DANS LE SYSTÈME

1. Le traitement des données dans le Système doit être limité à l'une ou à plusieurs des finalités en matière d'application de la loi suivantes :
   - **a.** prévention des infractions ;
   - **b.** enquête sur les infractions ;
   - **c.** détection des infractions ;
   - **d.** poursuite des infractions ;
   - **e.** exécution des sanctions ;
   - **f.** maintien de l'ordre public ;
   - **g.** protection contre les menaces à la sécurité publique et prévention de ces dernières ;
   - **h.** toute obligation ou responsabilité légale des services chargés de l'application de la loi.
2. Les données à caractère personnel collectées aux fins de l'application de la loi ne doivent pas être utilisées pour toute autre finalité incompatible avec la

finalité initiale à l'origine de leur collecte, sauf si cela est autorisé par la loi.

BONNES PRATIQUES

FINALITÉ DU TRAITEMENT

1. Respecter le périmètre défini conformément aux finalités en matière d'application de la loi
2. S'assurer de l'existence d'un texte de loi avant d'élargir le champ de la finalité du traitement
3. Éviter tout détournement de la finalité prévue

CHAPITRE III

RÉGIME DE PROTECTION DES DONNÉES ET GOUVERNANCE

3.1 CONTRÔLE ET NOTIFICATION

1. Chaque pays participant au SIPAO doit mettre en place une autorité de protection des données indépendante, conformément à l'article 14 de l'Acte additionnel.
2. Le Système doit être déclaré auprès de cette autorité conformément à la législation nationale du pays participant au SIPAO.
3. Si le pays participant au SIPAO n'a pas encore instauré la législation idoine ou l'autorité de protection des données indépendante requise, il est recommandé d'adopter les mesures suivantes : la publication de l'Acte additionnel de la CEDEAO dans le Journal Officiel et le respect des principes prévus par cet Acte. Il peut aussi mettre en place ou désigner un organisme de supervision indépendant qui assumera les fonctions de l'autorité de protection des données.
4. Chaque pays participant au SIPAO doit mettre en place un cadre juridique (sous la forme de lois, de règlements, de directives, de politiques, etc.) qui identifie clairement les services chargés de l'application de la loi responsables du traitement des données dans le Système et la manière dont les données à caractère personnel y seront traitées.
5. Un service chargé de l'application de la loi est responsable de toutes les opérations de traitement des données qu'il entreprend ou autorise, et il est tenu d'en rendre compte.

BONNES PRATIQUES

CONTRÔLE ET NOTIFICATION

1. Mettre en place une loi sur les données à caractère personnel et une autorité de protection des données indépendante conformément à l'article 14 de l'Acte additionnel

2. Procéder à la déclaration du Système auprès de l'autorité de protection des données indépendante

3. Sensibiliser les pouvoirs publics n'ayant pas encore instauré une législation sur les données à caractère personnel à l'urgence de publier l'Acte additionnel dans leur journal officiel

3.2 OFFICIER DÉLÉGUÉ À LA PROTECTION DES DONNÉES ET SENSIBILISATION ET FORMATION À LA PROTECTION DES DONNÉES

1. Chaque service chargé de l'application de la loi doit nommer un officier délégué à la protection des données. Ce dernier doit avoir une solide connaissance de la législation et des pratiques en matière de protection des données afin de réaliser les tâches suivantes :
   - **a.** informer et conseiller le service chargé de l'application de la loi traitant les données dans le Système des obligations légales qui lui incombent en matière de traitement des données à caractère personnel ;
   - **b.** contrôler la conformité du service chargé de l'application de la loi lors du traitement des données dans le Système ;
   - **c.** fournir des conseils sur les analyses d'impact relatives à la protection des données lorsque cela lui est demandé ;
   - **d.** coopérer et assurer la liaison avec les autorités de protection des données compétentes ;
   - **e.** mettre en œuvre, à l'intention des personnes travaillant avec le Système, des programmes de formation continue adaptés sur la protection des données.
2. Le cas échéant, l'officier délégué à la protection des données doit obtenir une certification et suivre une formation.
3. Les services chargés de l'application de la loi participant au programme SIPAO doivent s'assurer que l'ensemble des utilisateurs du Système bénéficient d'actions de sensibilisation et de formation à la protection des données.
4. L'officier délégué à la protection des données doit être suffisamment formé et/ou certifié pour gérer le cadre de protection des données du SIPAO.

BONNES PRATIQUES

OFFICIER DÉLÉGUÉ À LA PROTECTION DES DONNÉES

1. Nommer un officier délégué à la protection des données

2. Veiller à choisir un officier délégué à la protection des données qui présente le bon profil

3. Prévoir un programme de renforcement des capacités à l'intention de l'officier délégué à la protection des données et de l'ensemble des utilisateurs du Système

SUR LA FORMATION À LA PROTECTION DES DONNÉES DESTINÉE AUX SERVICES CHARGÉS DE L'APPLICATION DE LA LOI

Police de Dyfed Powys, action de l'ICO, réf. COM0666484, COM0672404, COM0677576

À la suite d'un audit, l'Information Commissioner's Office (ICO), l'autorité de protection des données du Royaume-Uni, a découvert que 1 204 des 2 258 officiers de police n'avaient pas suivi de formation à la protection des données, entraînant de nombreuses violations du Data Protection Act adopté par le Royaume-Uni. Ont notamment été relevées la transmission par un officier de police, sans la permission de la personne concernée, de données sensibles en utilisant un télécopieur en accès libre, et la diffusion par un autre d'une photographie de son bureau où l'on pouvait voir son écran et y lire des données sensibles et à caractère personnel. L'ICO a requis les actions suivantes :

- mise en place d'un programme de formation à la protection des données pour l'ensemble du personnel de police ;
- mise en place d'un programme de mise à niveau régulière destiné à l'ensemble du personnel de police afin de garantir le respect permanent du Data Protection Act ;
- mise en place d'un dispositif d'enregistrement et de suivi des programmes de formation ;
- application de toutes les autres mesures de sécurité pertinentes pour protéger les données à caractère personnel de tout traitement non autorisé et illicite, d'une perte accidentelle, d'une destruction et/ou de dommages.

Police du Humberside, action de l'ICO, réf. COM0649315

L'ICO a réalisé un audit au sein de la police du Humberside après un incident impliquant la perte de disques non cryptés contenant l'audition d'une victime présumée de viol. Selon les conclusions de l'audit, le Département ne s'est conformé à son obligation d'assurer une formation de son personnel en protection des données qu'à un taux de 16,8 %. Le responsable du traitement a donc pris les mesures nécessaires pour s'assurer que :

- tous les membres du personnel chargés de traiter des données à caractère personnel reçoivent, dans les six mois, une formation adaptée et spécifique sur la protection des données ;
- tous les membres du personnel qui travaillent régulièrement avec des supports amovibles comme des CD, des DVD et des clés USB reçoivent une formation sur l'utilisation du cryptage, notamment dans les cas de figure nécessitant le cryptage des données, et comment y procéder ;

- des programmes annuels de mise à niveau sont suivis ;
- les nouveaux membres du personnel chargés de traiter des données à caractère personnel reçoivent une formation adaptée et spécifique sur la protection des données lors de leur intégration ;
- la participation au programme de formation fait l'objet d'un suivi ;
- les politiques et les procédures établies par l'autorité de protection des données sont communiquées et mises à la disposition du personnel chargé du traitement des données à caractère personnel au sein de chaque département.

3.3 RESPECT DES PRINCIPES DE PROTECTION DES DONNÉES ET GOUVERNANCE

1. Afin de garantir le respect des principes en matière de protection des données dans le cadre de la mise en œuvre et de l'utilisation du SIPAO, les services chargés de l'application de la loi concernés doivent traiter toutes les données à caractère personnel de façon à minimiser les risques associés à un traitement non autorisé et illicite.
2. Les services chargés de l'application de la loi doivent intégrer la protection des données et de la vie privée des individus afin d'aligner les exigences des principes en matière de protection des données sur celles de leurs objectifs et culture organisationnels. Cela passe par la compréhension de ces principes et de leur champ d'application, l'identification des lacunes en matière de conformité constatées à l'échelle de l'organisation, la création de plans pour y remédier et la mise en œuvre stratégique des plans, des politiques et des procédures.
3. Les services chargés de l'application de la loi doivent aussi mettre en œuvre des politiques en vue d'attribuer au personnel ou aux salariés des responsabilités claires en matière de protection des données et de les responsabiliser.
4. Les interventions stratégiques de gouvernance susceptibles de faciliter la mise en œuvre des principes peuvent inclure les actions suivantes :
   a. Confier à une personne spécifique la responsabilité de la protection des données dans le cadre de la mise en œuvre et de l'utilisation du SIPAO (par ex., l'officier délégué à la protection des données). Cette personne doit gérer au jour le jour les questions relatives à la protection des données dans le SIPAO. Elle peut appartenir à une fonction dédiée à la protection des données ou faire partie des directions juridique, conformité, informatique, sécurité ou gestion des informations.
   b. Sensibiliser et impliquer les hautes autorités des services chargés de l'application de la loi dans la gestion du cadre de protection des données du SIPAO. La mise en œuvre d'un cadre de protection des données requiert la participation du personnel de direction afin d'en faciliter le processus. Cet appui institutionnel peut revêtir les formes suivantes :

i. sensibilisation de l'ensemble du personnel et des niveaux de direction inférieurs à l'importance de la protection des données au sein du Système ;
ii. implication et participation aux initiatives portant sur la gestion des données ;
iii. déblocage du financement nécessaire pour soutenir les activités de protection des données.

c. Rendre le service chargé de l'application de la loi responsable du cadre de protection des données du SIPAO. À quelques rares exceptions, la gestion de la protection des données requerra la contribution et la participation de toutes les personnes utilisant le SIPAO. L'officier délégué à la protection des données peut donc constituer une équipe de protection des données qui interviendra au sein des différents groupes fonctionnels afin de mieux les informer sur les risques encourus en matière de protection des données.

d. Assurer des échanges réguliers entre l'officier délégué à la protection des données, l'équipe de protection des données et les autres responsables de la protection des données au sein du SIPAO. Cela peut faciliter la mise en œuvre efficace du cadre de protection des données pour :

i. apporter un soutien proactif afin que la protection des données soit intégrée aux projets en cours ;
ii. aider les utilisateurs à réaliser leurs objectifs.

e. Faire participer toutes les parties prenantes clés au cadre de protection des données du SIPAO. L'officier délégué à la protection des données doit entretenir des échanges avec les utilisateurs du Système. La participation des parties prenantes clés peut se manifester par des discussions ou des réunions formelles (mensuelles ou trimestrielles) consacrées au cadre de protection des données du SIPAO. L'officier délégué à la protection des données doit aussi être impliqué dans les activités susceptibles d'avoir des répercussions sur la protection des données comme la sécurité informatique, les enquêtes, le recueil de renseignements, etc.

f. Produire régulièrement des rapports internes à la hiérarchie portant sur les risques, les violations de données ou les événements majeurs liés à la protection des données. Ces rapports doivent mettre en évidence les principaux risques en matière de protection des données, les violations de données ou événements, etc. Des rapports précis et exacts sur la confidentialité et la protection des données aux personnes chargées de superviser et de gérer le cadre de protection des données sont essentiels pour garantir que les autorités chargées de l'application de la loi utilisant le SIPAO se mettent en conformité et pour réduire les risques liés à la non-conformité. À cette fin, il est important d'envisager d'élaborer des indicateurs de mesure relatifs à la conformité, à la mise en œuvre et au compte-rendu.

g. Faire des rapports aux parties prenantes externes telles que les autorités de protection des données, les autorités publiques, d'autres services chargés de l'application de la loi et d'autres parties prenantes clés, le cas échéant. La sensibilisation externe à la mise en œuvre du cadre de protection des données est essentielle pour garantir l'ouverture et la transparence. Favoriser la sensibilisation externe de toutes les parties prenantes clés renforce également l'intégrité et donne une confiance dans le Système. Les services chargés de l'application de la loi utilisant le SIPAO doivent s'efforcer d'adopter une approche centrée sur l'utilisateur et de faire de la transparence une priorité en explorant des moyens plus appropriés de remplir leurs obligations. L'utilisation d'un langage simple est encouragée. La sensibilisation externe peut être réalisée par le biais de moyens tels que :

i. des rapports sur la transparence émis par le service chargé de l'application de la loi ;
ii. le dépôt des rapports d'audit sur le respect de la protection des données auprès de l'autorité de protection des données (si elle a été mise en place) ;
iii. la publication des rapports d'audit sur le respect de la protection des données ;
iv. la réalisation d'audits de vérification ou de responsabilité par des tiers ;
v. la création et la gestion d'un avis de protection des données.

h. Évaluer les risques en matière de protection des données au sein de l'ensemble des unités ou départements qui accèdent au SIPAO. Cette évaluation doit être une condition préalable à tout développement d'une politique globale de protection des données. L'officier délégué à la protection des données doit élaborer des autoévaluations portant sur la protection des données au sein des unités ou des départements, passer en revue les procédures, y apporter des améliorations, dispenser des communications et des formations relatives au SIPAO et superviser toutes ces actions. Le processus d'évaluation des risques lui permettra d'identifier et de prioriser les lacunes en matière de protection des données au sein du service chargé de l'application de la loi et de gérer la mise en œuvre de la politique d'atténuation des risques au sein du SIPAO. Le cas échéant, les services chargés de l'application de la loi peuvent envisager de faire appel à un tiers compétent pour les aider.

i. Demander à l'ensemble du personnel SIPAO d'attester avoir pris connaissance du cadre de protection des données du SIPAO et de s'engager à le respecter. Cela est nécessaire pour que les salariés ou le personnel comprennent bien l'importance de la protection des données dans le cadre de la mise en œuvre et de l'utilisation du SIPAO. Il est important de responsabiliser les salariés ou le personnel au titre de leurs actes en matière de traitement

des données à caractère personnel. Chaque salarié doit donc attester avoir pris connaissance du cadre de protection des données et s'engager à le respecter. Cette reconnaissance et cet engagement peuvent être formulés dans un document séparé (papier ou électronique) ou être intégrés à un document existant, comme les conditions de service, le code de conduite, un guide du salarié ou un exemplaire de la politique de protection des données.

BONNES PRATIQUES

RÉGIME DE PROTECTION DES DONNÉES ET GOUVERNANCE

1. Minimiser les risques liés au traitement non autorisé ou illicite dans le Système
2. Définir et préciser les rôles et responsabilités de chaque intervenant dans le Système
3. Sensibiliser et impliquer les hautes autorités des services chargés de l'application de la loi dans la gestion du cadre de protection des données du SIPAO
4. Promouvoir un réseau d'échange entre les intervenants dans le Système
5. Produire des rapports sur la protection des données liés au fonctionnement du Système
6. Évaluer les risques en matière de protection des données au sein de l'ensemble des unités ou départements qui accèdent au SIPAO
7. Faire signer à chaque intervenant une déclaration relative à la protection des données dans le Système

CHAPITRE IV

COLLECTE ET PARTAGE DES DONNÉES À CARACTÈRE PERSONNEL

4.1 COLLECTE DES DONNÉES À CARACTÈRE PERSONNEL

1. Les services chargés de l'application de la loi doivent s'assurer de l'existence d'un fondement juridique avant de procéder à la collecte des données à caractère personnel.
2. La collecte des données à caractère personnel dans le Système doit être limitée à ce qui est nécessaire et proportionnel aux finalités en matière d'application de la loi pour lesquelles elles sont collectées.

ÉTUDE DE CAS

SUR LA NÉCESSITÉ DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Affaire Uzun c. Allemagne, arrêt de la CEDH, 2 septembre 2010, requête No 35629/05

Le requérant, suspecté d'être impliqué dans un attentat à la bombe commis par un mouvement d'extrême gauche, a allégué que les mesures de surveillance, en particulier par GPS, dont il avait fait l'objet et l'utilisation des informations ainsi obtenues dans le cadre de la procédure pénale dirigée contre lui avaient emporté violation de ses droits et protections garantis par l'article 8 de la Convention de la CEDH (droit au respect de la vie privée).

Tout en reconnaissant que la surveillance par GPS est, par nature, plus susceptible d'ingérer avec le droit au respect de la vie privée d'une personne (article 8), la Cour a estimé qu'une telle ingérence était acceptable lorsque ces mesures sont « nécessaires dans une société démocratique ». La surveillance par GPS n'a pas été recherchée ou accordée d'emblée, mais uniquement après plusieurs mois de surveillance visuelle et l'épuisement d'autres mesures moins intrusives. De plus, la surveillance par GPS n'a affecté le requérant que lorsqu'il se trouvait dans son véhicule, et il ne pouvait donc prétendre avoir été soumis à une surveillance totale et exhaustive. Enfin, la surveillance ayant été conduite dans le cadre d'une menace publique grave (tentatives de meurtre d'hommes politiques et de fonctionnaires par des attentats à la bombe), elle a été « nécessaire » au sens de l'article 8.

3. Lorsque des données à caractère personnel sont collectées, il est nécessaire d'établir une relation claire entre la personne dont les données à caractère personnel sont traitées et la finalité du traitement.

SUR LA RELATION ENTRE LES DONNÉES À CARACTÈRE PERSONNEL ET LA PERSONNE CONCERNÉE

Affaire Mustafa Sezgin Tanrikulu c. Turquie, arrêt de la CEDH, 18 juillet 2017, requête No 27473/06

À la suite d'un attentat à la bombe qui a tué un inspecteur de police, le service du renseignement de la Turquie (« MIT ») a obtenu une ordonnance judiciaire afin d'intercepter l'ensemble des appels et des communications téléphoniques nationaux et internationaux réalisés entre le 8 avril et le 30 mai 2005 par Turk Telekom, les opérateurs de réseaux mobiles privés et les fournisseurs d'accès internet du pays afin d'obtenir les informations contenues dans les communications SMS, MMS, GPRS et par télécopie, ainsi que l'identité des appelants, les adresses IP et toutes les autres informations afférentes aux communications.

La CEDH a estimé que cette ordonnance, qui a autorisé l'interception des communications de toutes les personnes se trouvant sur le territoire de la République de Turquie, était illicite, car elle n'était notamment pas limitée aux personnes suspectées d'infractions pénales, comme cela est requis par la législation applicable.

4. Les services chargés de l'application de la loi doivent faire une distinction claire entre les différentes catégories de personnes concernées dont les données sont traitées, comme les suspects, les personnes d'intérêt dans le cadre d'une enquête, les personnes reconnues coupables d'une infraction pénale, les victimes, les témoins, les contacts des différentes personnes mentionnées, etc.
5. Les services chargés de l'application de la loi doivent s'assurer que les données collectées sont exactes, ne sont pas trompeuses, sont à jour, adéquates, pertinentes et non excessives au regard des finalités de leur traitement.

BONNES PRATIQUES

COLLECTE DES DONNÉES

1. S'assurer de l'existence d'un fondement juridique avant de procéder à la collecte des données à caractère personnel
2. Respecter le principe de proportionnalité lors de la collecte des données à caractère personnel
3. S'assurer que les données collectées sont exactes, ne sont pas trompeuses, sont à jour, adéquates, pertinentes et non excessives au regard des finalités de leur traitement

4.2 PARTAGE OU TRANSMISSION DES DONNÉES À D'AUTRES ORGANISMES PUBLICS

1. Les services chargés de l'application de la loi peuvent partager ou transmettre des données à caractère personnel à d'autres organismes publics qui ne sont pas des services chargés de l'application de la loi si :
   a. ce partage et cette transmission sont prévus par la loi ;
   b. les données sont demandées par le destinataire afin de lui permettre de mener une tâche légale (par exemple, dans le cadre d'enquêtes ou d'autres obligations légales conformément au droit national) ou de prévenir un risque grave et imminent pour des tiers, l'ordre public ou la sécurité publique.
2. Lorsqu'ils évaluent la nécessité de partager ou de transmettre des données à d'autres organismes publics, les services chargés de l'application de la loi doivent identifier le préjudice qu'une telle transmission peut causer aux personnes concernées.
3. Les services chargés de l'application de la loi doivent informer l'organisme public destinataire de son obligation d'utiliser les données partagées ou transmises uniquement pour les finalités pour lesquelles elles sont partagées ou transmises.
4. Les services chargés de l'application de la loi doivent s'assurer que les organismes publics ont pris les mesures nécessaires pour respecter le cadre de protection des données applicable.

PARTAGE DES DONNÉES

1. S'assurer de l'existence d'une loi avant de partager ou transmettre des données à d'autres organismes
2. Identifier les éventuels préjudices qui peuvent impacter une personne avant de partager ou transmettre des données à d'autres organismes
3. Informer l'organisme public destinataire des données de l'obligation de respecter les finalités pour lesquelles les données ont été partagées ou transmises

4.3 PARTAGE OU TRANSMISSION DES DONNÉES À DES ORGANISMES PRIVÉS OU AU GRAND PUBLIC

1. Conformément à la législation en vigueur dans chaque pays, les services chargés de l'application de la loi peuvent partager ou transmettre des données à caractère personnel à des organismes privés dans l'un ou plusieurs des cas suivants :
   - **a.** pour réaliser les finalités en matière d'application de la loi ;
   - **b.** pour prévenir un risque grave et imminent pour l'ordre public ou la sécurité publique ;
   - **c.** dans l'intérêt des personnes concernées ;
   - **d.** pour des raisons humanitaires.
2. Lorsqu'ils évaluent la nécessité de partager ou de transmettre des données à caractère personnel à des organismes privés, les services chargés de l'application de la loi doivent identifier le préjudice qu'une telle transmission peut causer aux personnes concernées.
3. Lorsque des données à caractère personnel sont partagées ou transmises à un organisme privé, le service chargé de l'application de la loi concerné doit veiller à ce que celui-ci s'engage par écrit à respecter les principes applicables en matière de protection des données.
4. Lorsqu'ils partagent ou transmettent des données à caractère personnel au grand public dans le cadre de la divulgation d'informations afférentes à une enquête, les services chargés de l'application de la loi doivent s'interroger sur la nécessité et l'intérêt public d'un tel partage ou d'une telle transmission. Des garanties idoines doivent être prises afin que les droits des personnes physiques concernées par l'affaire soient respectés.
5. Le partage ou la transmission de données au grand public ne doivent être effectués qu'aux fins :
   - **a.** de l'alerter ;

b. de solliciter son aide ; ou

c. de réaliser toute autre finalité en matière d'application de la loi définie au point 2.2 ci-dessus.

6. Si un service chargé de l'application de la loi a reçu des données à caractère personnel d'un autre service chargé de l'application de la loi, il doit requérir l'autorisation formelle du service expéditeur avant de partager ou de transmettre ces données à caractère personnel à un organisme privé ou au grand public.

7. Le service chargé de l'application de la loi qui procède au partage ou à la transmission doit prendre les mesures nécessaires pour garantir le même niveau de protection, ou un niveau de protection supérieur, des données à caractère personnel partagées ou transmises.

BONNES PRATIQUES

PARTAGE OU TRANSMISSION DES DONNÉES À DES ORGANISMES PRIVÉS OU AU GRAND PUBLIC

1. Respecter les conditions fixées par les textes avant de partager ou de transmettre des données à caractère personnel à des organismes privés
2. Identifier les préjudices pouvant être causés aux victimes ou témoins avant de partager ou de transmettre des données à caractère personnel à des organismes privés
3. Informer les victimes et les témoins avant de partager ou de transmettre des données à caractère personnel au grand public
4. Respecter les droits des personnes physiques en cas de partage ou de transmission des données à caractère personnel au grand public
5. Requérir l'autorisation formelle du service chargé de l'application de la loi avant de partager ou de transmettre des données à caractère personnel à un organisme privé ou au grand public
6. S'assurer de l'existence d'un niveau de protection adéquate des données auprès du destinataire avant de partager ou de transmettre des données à caractère personnel à des organismes privés ou publics
7. Faire signer par les organismes privés un engagement écrit relatif au respect des principes applicables en matière de protection des données

SUR LA TRANSMISSION DE DONNÉES À CARACTÈRE PERSONNEL À DES MEMBRES DU GRAND PUBLIC

Police des Midlands de l'Ouest, action de l'ICO, réf. ENF0674010

Une ordonnance de comportement criminel (CBO) pour atteintes aux biens d'autrui et menaces de violence a été imposée à deux individus. Elle leur interdisait de pénétrer dans certains endroits et de se réunir dans certains lieux. La police des Midlands de l'Ouest (responsable du traitement) a décidé de rendre publics les termes de cette ordonnance par le biais d'un prospectus distribué dans la région. Les prospectus ont été élaborés et distribués auprès d'une trentaine de foyers et contenaient des données à caractère personnel sur les victimes et les témoins des infractions, reprises sans leur permission. L'ICO (autorité de protection des données) a demandé au responsable du traitement de veiller à ce que :

- des évaluations de risques relatifs aux victimes et aux témoins d'infractions soient réalisées dans le cadre des publications des CBO ;
- les victimes et les témoins soient informés avant la publication des supports ;
- la procédure de création et de distribution des supports soit documentée ;
- une formation obligatoire à la protection des données soit dispensée à tous les membres du personnel en place et nouvellement recrutés chargés de traiter les données à caractère personnel ;
- une mise à niveau en matière de protection des données soit dispensée à tous les membres du personnel chargés de traiter les données à caractère personnel ;
- des systèmes soient mis en place pour surveiller la participation aux formations à la protection des données ;
- la mise en œuvre ait lieu dans les trois mois.

4.4 PARTAGE OU TRANSMISSION DES DONNÉES AU NIVEAU INTERNATIONAL

1. En règle général, les services chargés de l'application de la loi qui partagent ou transmettent des données au niveau international doivent se demander si la fonction réalisée par le service destinataire lui est conférée par la loi à des fins d'application de la loi et si le partage des données est nécessaire pour qu'il réalise ses obligations en la matière. Le transfert international de données à caractère personnel est réservé uniquement aux services chargés de l'application de la loi.
2. Lors du partage ou de la transmission de données à caractère personnel à un service chargé de l'application de la loi d'un pays tiers ou à une organisation régionale ou internationale, le service qui partage ou transmet les données doit s'assurer que le pays et/ou le service chargé de l'application de la loi destinataire garantit un niveau de protection adéquat en matière de sécurité des informations, de respect de la vie privée, des libertés et des droits fondamentaux des personnes physiques dans le cadre du traitement desdites données.
3. Le service chargé de l'application de la loi qui procède au partage ou à la transmission des données doit prendre des mesures raisonnables pour garantir le même niveau de protection, ou un niveau de protection supérieur, des données partagées ou transmises.

BONNES PRATIQUES

PARTAGE OU TRANSMISSION INTERNATIONAL

1. Respecter les conditions fixées par les textes avant de partager ou de transmettre des données à caractère personnel au niveau international

2. S'assurer que le pays et/ou le service chargé de l'application de la loi destinataire garantit un niveau de protection adéquat dans le cadre du traitement desdites données

CHAPITRE V

QUALITÉ, CONFIDENTIALITÉ ET SÉCURITÉ DES DONNÉES

5.1 QUALITÉ DES DONNÉES

1. Les services chargés de l'application de la loi doivent prendre toutes les mesures raisonnables pour ne pas transmettre, partager ou mettre à disposition des données à caractère personnel qui sont inexactes, incomplètes ou obsolètes. À cette fin, ils doivent vérifier la qualité des données à caractère personnel avant leur transmission, leur partage ou leur mise à disposition.
2. Dans la mesure du possible, les informations nécessaires permettant au destinataire d'évaluer et de connaître le degré d'exactitude, d'exhaustivité et de fiabilité des données à caractère personnel, et de savoir dans quelle mesure elles sont à jour, doivent être jointes lors de toutes les transmissions ou de tous les partages desdites données.
3. Le destinataire doit être informé sans délai en cas de partage ou de transmission de données à caractère personnel inexactes ou incorrectes ou encore partagé ou transmis de manière illégale. Dans ce cas, les données à caractère personnel doivent être rectifiées, effacées ou traitées avec les restrictions adéquates.
4. Les données collectées doivent être classées en fonction de leur degré d'exactitude ou de fiabilité et, en particulier, les données factuelles doivent être isolées des données fondées sur des opinions ou des évaluations personnelles.

ÉTUDE DE CAS

SUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL INCORRECTES

Affaire Cemalettin Canli c. Turquie, arrêt de la CEDH, 18 novembre 2008, requête No 22427/04

En 2003, alors qu'une procédure pénale était en cours contre M Canli, les autorités policières ont soumis un rapport de police mentionnant deux autres procédures pénales datant de 1990 et l'impliquant du fait de son appartenance à une organisation illégale. M. Canli avait été acquitté dans le cadre de l'une, tandis que l'autre avait été classée sans suite.

La Cour a déclaré que ce rapport de police n'était pas conforme à la loi puisqu'il ne mentionnait pas l'acquittement de M. Canli dans la première affaire et le classement sans suite de la deuxième procédure pénale.

Affaire Mikolajova c. Slovaquie, arrêt de la CEDH, 18 janvier 2011, requête no 4479/03

En 2000, l'époux de la requérante a déposé une plainte pénale à son encontre alléguant qu'elle l'avait agressé. Les accusations ont été abandonnées quelques jours plus tard et la plainte n'a jamais été portée devant les tribunaux ni donné lieu à une condamnation. Toutefois, la police a noté dans le dossier de la requérante qu'elle avait commis une infraction pénale en infligeant des blessures corporelles à autrui et a communiqué ces informations à un tiers, qui les a utilisées au détriment de la requérante. La Cour a déclaré que la décision de la police avait violé les droits de la requérante, car sa culpabilité était affirmée, alors même qu'elle n'avait jamais été condamnée ni reconnue coupable de l'infraction.

BONNES PRATIQUES

QUALITÉ DES DONNÉES

1. Veiller à la qualité des données avant leur transmission, leur partage ou leur mise à disposition

2. Informer les parties prenantes en cas de transmission, partage ou mise à disposition de données inexactes ou incorrectes

3. Classer les données collectées en fonction de leur degré d'exactitude ou de fiabilité

5.2 CONFIDENTIALITÉ ET SÉCURITÉ

1. Les services chargés de l'application de la loi doivent prendre des mesures adaptées, raisonnables, techniques et organisationnelles pour sécuriser le Système contre les risques liés à l'accès, la destruction, la perte, l'utilisation, la modification ou la divulgation accidentels ou non autorisés des données à caractère personnel.
2. Les services chargés de l'application de la loi doivent déployer des mesures visant à :
   - **a.** empêcher toute personne non autorisée à accéder à l'équipement du Système utilisé pour le traitement des données ;
   - **b.** empêcher que les données puissent être lues, copiées, modifiées ou supprimées du Système ;
   - **c.** empêcher l'introduction non autorisée de données à caractère personnel, ainsi que la consultation, la modification ou l'effacement non autorisés de données à caractère personnel enregistrées ;
   - **d.** empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données ;
   - **e.** garantir que les personnes autorisées à utiliser le Système ne peuvent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation d'accès ;
   - **f.** garantir la possibilité de vérifier et constater à quelles instances des données à caractère personnel enregistrées dans le Système ont été ou peuvent être transmises ou mises à disposition ;
   - **g.** garantir la possibilité de vérifier et constater a posteriori quelles données à caractère personnel ont été introduites dans le Système, et à quel moment et par quelle personne elles y ont été introduites ;
   - **h.** empêcher que, lors des transferts de données à caractère personnel ou lors du transport des supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée ;
   - **i.** garantir qu'en cas d'interruption, il est possible de rétablir rapidement le Système ;
   - **j.** garantir que les fonctions du Système sont opérationnelles, que les erreurs de fonctionnement sont signalées et que les données à caractère personnel conservées ne peuvent être corrompues par un dysfonctionnement du Système.
3. Les données communiquées à des sous-traitants ou gérées par ces derniers doivent bénéficier de garanties suffisantes, notamment en matière de confidentialité des données personnelles.

ÉTUDE DE CAS

SUR LA DIVULGATION ACCIDENTELLE DE DONNÉES À CARACTÈRE PERSONNEL

Police du Gloucestershire, amende de l'ICO, 11 juin 2018

Le 19 décembre 2016, un officier de police qui enquêtait sur des affaires d'abus pédosexuels anciens a envoyé un courriel à 56 destinataires sans utiliser la fonction copie cachée, permettant à tous ceux-ci (on estime qu'au moins 52 personnes ont bien reçu le courriel) de voir les adresses électroniques des victimes, des journalistes et des avocats. Le courriel a été rappelé le 21 décembre 2016, et l'affaire a été portée devant l'ICO (autorité de protection des données). Pour cette dernière :

- la police n'a pas envoyé de courriels séparés à chaque destinataire et a utilisé la fonction d'envoi groupé ;
- la police n'a pas utilisé la fonction copie cachée de Microsoft Outlook ;
- la police n'a pas communiqué à son personnel des politiques ou directives suffisantes sur l'envoi groupé de courriels et sur l'utilisation de la fonction copie cachée d'Outlook, ni ne lui a fait suivre de formation adéquate sur ces sujets, en particulier dans des affaires où les courriels ont été envoyés à de nombreuses victimes d'affaires sensibles ou en cours ;
- la police a immédiatement contacté les personnes concernées et l'autorité de protection des données comme requis.

L'ICO a donc imposé une amende de 80 000 livres sterling après la prise en compte de certains facteurs atténuants, notamment le fait que la police a averti les personnes concernées rapidement, que plusieurs des destinataires étaient déjà au courant, que l'ICO a été averti rapidement et que la police du Gloucestershire est en train de renforcer ses mesures techniques et organisationnelles afin que de tels cas ne se reproduisent pas.

ÉTUDE DE CAS

SUR L'INTRODUCTION DE DONNÉES À CARACTÈRE PERSONNEL À DES FINS MALVEILLANTES

CNBC, « Un officier de l'immigration licencié après avoir inscrit son épouse sur la liste des terroristes afin de l'empêcher de rentrer chez elle », 1er février 2011

Un officier de l'immigration britannique a essayé de se débarrasser de son épouse en inscrivant son nom sur une liste de personnes suspectées de terrorisme. Il s'est servi de son accès aux bases de données de sécurité pour l'inscrire sur la liste des personnes à surveiller interdites d'embarquement vers la Grande-Bretagne, car leur présence dans le pays n'est « pas propice au bien public ». De ce fait, pendant trois ans, son épouse n'a pu rentrer du Pakistan où elle était partie rendre visite à sa famille. L'altération de la liste des personnes suspectées de terrorisme est restée inaperçue jusqu'à ce que cet officier soit retenu pour une promotion et que le nom de son épouse y soit retrouvé au cours d'une enquête de vérification. Le *Home Office* britannique a confirmé que l'officier avait été licencié pour faute grave.

BONNES PRATIQUES

CONFIDENTIALITÉ ET SÉCURITÉ

1. Veiller à l'intégrité du Système
2. Mettre en place une politique de sécurité
3. Assurer la confidentialité des données du Système
4. Respecter l'obligation de notification des failles en cas d'atteinte au Système
5. Prendre des mesures d'urgence techniques et organisationnelles en cas d'atteinte au Système

CHAPITRE VI

VIOLATIONS DE DONNÉES

6.1 NOTIFICATION DES VIOLATIONS DE DONNÉES

1. Les services chargés de l'application de la loi doivent répertorier toutes les violations de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.
2. Si une violation de données à caractère personnel est susceptible d'engendrer un risque pour les droits et libertés de personnes physiques, les services chargés de l'application de la loi, par le biais de leur officier délégué à la protection des données, doivent en avertir l'autorité de protection des données sans délai et, dans la mesure du possible, au plus tard dans les 72 heures après en avoir eu connaissance. La notification de la violation de données à l'autorité de protection des données doit :
   a. décrire la nature de la violation de données à caractère personnel, y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
   b. communiquer le nom et les coordonnées de l'officier délégué à la protection des données ou d'un autre point de contact pouvant fournir des informations supplémentaires ;
   c. décrire les conséquences probables de la violation de données à caractère personnel ; et
   d. décrire les mesures prises, ou que le responsable du traitement propose de prendre, pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
3. Si un service chargé de l'application de la loi a partagé ou transmis des données à un destinataire basé dans un autre pays, les informations du point 2 cidessus doivent lui être communiquées.

6.2 NOTIFICATION DES VIOLATIONS DE DONNÉES AUX PERSONNES CONCERNÉES

1. Si une violation de données à caractère personnel est susceptible d'engendrer un risque pour les droits et libertés de personnes physiques, les services chargés de l'application de la loi concernés doivent en avertir les personnes concernées sans délai. Le service chargé de l'application de la loi doit :
   a. communiquer le nom et les coordonnées de l'officier délégué à la protection des données ou d'un autre point de contact pouvant fournir des informations supplémentaires aux personnes concernées ;

b. décrire les conséquences probables de la violation de données à caractère personnel ;

c. décrire les mesures prises ou à prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

2. Cette communication aux personnes concernées n'est pas requise si :

a. le service chargé de l'application de la loi a mis en œuvre des mesures de protection techniques et organisationnelles appropriées et si ces dernières ont été appliquées aux données à caractère personnel affectées par la violation de données, en particulier des mesures qui les rendent incompréhensibles pour toute personne n'étant pas autorisée à y avoir accès, comme le chiffrement ;

b. le service chargé de l'application de la loi a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;

c. elle exigerait des efforts disproportionnés. Dans ce cas, le service chargé de l'application de la loi doit plutôt procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

3. La communication aux personnes concernées peut être retardée, limitée ou omise lorsque, en tenant dûment compte de leurs droits fondamentaux et de leurs intérêts légitimes, cela constitue une mesure nécessaire et proportionnée pour :

a. éviter d'entraver des recherches, des enquêtes ou des procédures officielles ou judiciaires ;

b. éviter de nuire à la prévention, à la détection, aux enquêtes et aux poursuites d'infractions pénales, ou à l'exécution de sanctions pénales ;

c. protéger la sécurité publique ;

d. protéger la sécurité nationale ;

e. protéger les droits et libertés de tiers.

ÉTUDE DE CAS

SUR LA NOTIFICATION D'UNE VIOLATION DE DONNÉES AUX PERSONNES CONCERNÉES ET À L'AUTORITÉ DE PROTECTION DES DONNÉES

Crown Prosecution Service, amende de l'ICO, 14 mai 2018

La police a envoyé au CPS (Crown Prosecution Service, le Parquet britannique) des DVD contenant des auditions de victimes d'abus pédosexuels. L'absence de ces DVD a été constatée après leur livraison au CPS. Tant les personnes concernées que l'ICO (l'autorité de protection des données) ont été informées. Les DVD n'étaient pas cryptés, même si le CPS aurait pu y procéder, ni expédiés dans un conditionnement inviolable. Pour l'autorité de protection des données :

- le CPS n'a pas provoqué intentionnellement la perte des DVD, mais aurait dû savoir qu'il existait un risque de perte ;
- le CPS a déjà géré ce type d'auditions par le passé et a déjà été l'auteur d'une violation similaire en raison de son incapacité à sécuriser correctement les enregistrements de victimes et de témoins dans des affaires d'abus sexuels ;
- le CPS a été incapable de prendre des mesures raisonnables pour empêcher la perte, comme le transport de DVD cryptés dans un conditionnement scellé, inviolable, confié à une entreprise de messagerie sûre, avec remise contre signature, et le placement des DVD livrés dans un lieu sûr ;
- le CPS n'a pas immédiatement averti les personnes concernées ;
- le CPS n'a pas immédiatement averti l'autorité de protection des données comme il aurait dû le faire ;
- le CPS a tardé à faire remonter le problème aux niveaux adéquats ;
- les DVD n'ont toujours pas été retrouvés.

L'ICO a imposé une amende de 200 000 livres sterling.

BONNES PRATIQUES

NOTIFICATION DES VIOLATIONS

1. Avertir l'autorité de protection des données et les personnes concernées en cas de violation de données

2. Informer l'autorité de protection des données et les personnes concernées des mesures prises ou à prendre pour remédier à la violation de données à caractère personnel

3. Notifier sans retard indu les personnes concernées et l'autorité de protection des données

CHAPITRE VII

TRAITEMENT DES REGISTRES ET CONSERVATION DES DONNÉES

7.1 REGISTRES DES ACTIVITÉS DE TRAITEMENT

1. Les services chargés de l'application de la loi doivent conserver des registres de toutes les activités de traitement effectuées sous leur responsabilité avec :
   - **a.** le nom et les coordonnées de la ou des personnes en charge du Système dans le pays et de l'officier délégué à la protection des données ;
   - **b.** la finalité du traitement ;
   - **c.** les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
   - **d.** une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
   - **e.** le cas échéant, le recours au profilage ;
   - **f.** le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
   - **g.** une indication du fondement juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées ;
   - **h.** dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données à caractère personnel ;
   - **i.** dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles applicables au Système.

7.2 JOURNAUX

1. Les services chargés de l'application de la loi doivent conserver des journaux sur les opérations de traitement suivantes :
   - **a.** collecte ;
   - **b.** modification ;
   - **c.** accès/consultation ;
   - **d.** communication, y compris les transferts ;
   - **e.** interconnexion ;
   - **f.** effacement.
2. En cas de consultation ou de communication, les journaux des opérations de traitement doivent permettre d'établir le motif, la date et l'heure de cellesci et d'identifier la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires desdites données.
3. Les journaux doivent être utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de sécurité des

données à caractère personnel et aux fins des procédures pénales. Les services chargés de l'application de la loi doivent mettre les journaux à la disposition de l'autorité de protection des données sur demande.

4. Seule une personne ayant le rôle agréé « d'auditeur » dans le Système peut évaluer les journaux et ne peut le faire qu'en utilisant ce dernier.
5. Les journaux peuvent être modifiés ou effacés conformément aux politiques et/ou aux bonnes pratiques acceptables.

7.3 CONSERVATION DES DONNÉES

1. Les services chargés de l'application de la loi doivent élaborer des règles et/ou des recommandations internes définissant la période de conservation des données à caractère personnel ou revoir à intervalles réguliers la nécessité de conserver les données à caractère personnel.
2. Les services chargés de l'application de la loi doivent réévaluer périodiquement les motifs de la conservation et du traitement des données à caractère personnel.
3. Afin de déterminer la période adéquate de conservation des données à caractère personnel dans le Système, les services chargés de l'application de la loi doivent :
   a. examiner la durée de conservation des données à caractère personnel en se fondant sur la législation en vigueur dans chaque pays, la nature des données, leurs politiques et les bonnes pratiques ;
   b. considérer la finalité spécifique des informations avant de décider de conserver des données à caractère personnel (et leur période de conservation) ;
   c. effacer de façon sécurisée les informations lorsqu'elles ne sont plus nécessaires aux finalités spécifiées ;
   d. actualiser, archiver ou effacer de manière sécurisée les informations obsolètes.
4. Les données traitées dans le Système ne doivent être conservées que le temps nécessaire pour permettre aux services concernés de remplir leur mission.

ÉTUDE DE CAS

SUR LA CONSERVATION DES DONNÉES

Affaire Brunet c. France, arrêt de la CEDH, 18 août 2014, requête No 21010/10

M. Brunet et sa compagne ont eu une violente altercation et celui-ci a été placé en garde à vue. Sa compagne et lui ont écrit au procureur de la République pour exprimer leur désaccord quant à la qualification de l'infraction et la procédure judiciaire a été classée sans suite. Toutefois, les données à caractère personnel de M. Brunet ont été conservées dans le système de traitement des infractions constatées (STIC) de la police française en lien avec l'altercation et devaient y être conservées pendant 20 ans. Après plusieurs tentatives infructueuses du requérant de faire effacer ses informations du STIC, le procureur l'a informé qu'il n'avait pas la capacité de déterminer si les données pouvaient être effacées de ce système.

La Cour a déclaré que, puisque le STIC contient des informations sur l'identité et la personnalité de personnes physiques aux fins des recherches sur les infractions, y conserver les informations de M. Brunet pendant 20 ans constituait une mesure excessive, en particulier du fait que les accusations avaient été abandonnées et qu'aucune poursuite judiciaire n'avait été entamée. De plus, il n'avait pas eu de réelle opportunité de demander l'effacement de ses données, le procureur n'ayant pas la capacité de déterminer le caractère fondé de leur conservation.

BONNES PRATIQUES

CONSERVATION DES DONNÉES

1. Élaborer des règles et/ou des recommandations internes définissant la période de conservation des données à caractère personnel ou pour un examen périodique de la nécessité du stockage des données personnelles

2. Les autorités chargées de l'application de la loi doivent réévaluer périodiquement les motifs de la conservation et du traitement des données à caractère personnel

3. Veiller à ne conserver les données que le temps nécessaire pour permettre aux services concernés de remplir leur mission

CHAPITRE VIII

TRAITEMENT DES DONNÉES SENSIBLES

8.1 TRAITEMENT DES DONNÉES SENSIBLES

1. Les données à caractère personnel qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'orientation sexuelle, ainsi que les données génétiques ou plus généralement les données sur l'état de santé d'une personne physique (les « données sensibles ») ne doivent être traitées dans le Système qu'en cas de nécessité absolue, sous réserve de garanties appropriées au titre des droits et libertés de la personne concernée, et uniquement :
   - **a.** lorsque le traitement est autorisé par le droit de la CEDEAO ou celui du pays participant au SIPAO ;
   - **b.** pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou
   - **c.** lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

ÉTUDE DE CAS

SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL SENSIBLES

Police du Humberside, amende de l'ICO, 28 mars 2018

La police du Humberside a perdu trois disques contenant l'audition d'une victime présumée de viol. Les disques étaient la seule copie et contenaient des données sensibles et à caractère personnel sur la victime présumée et sur l'auteur présumé, notamment leur nom complet, leur date de naissance, ainsi que des informations sur l'état de santé mental et le traitement suivi par la victime présumée. Les seules notes écrites détaillant l'audition se trouvaient avec les disques. L'absence des disques n'a été découverte que 14 mois après l'audition. La victime a été avertie et n'a pas souhaité participer à d'autres auditions avec la police. Les disques n'ont jamais été retrouvés. Pour l'autorité de protection des données :

- la police a manqué de procéder au cryptage des disques pour les transférer en dehors de sa circonscription ;
- la police a manqué de réaliser des copies fonctionnelles des disques avant de les transférer en dehors de sa circonscription ;

- la police a manqué de respecter les politiques relatives à la sécurité des informations en vigueur ;
- la police a manqué de maintenir une piste d'audit des différents lieux de conservation des disques ;
- la police a manqué de fournir une formation adéquate sur la protection des données à ses officiers et de mettre en place un programme de suivi suffisant ;
- la police a manqué de renforcer les politiques et procédures existantes en matière de stockage et de transfert de données.

L'ICO a imposé une amende de 130 000 livres sterling.

BONNES PRATIQUES

TRAITEMENT DES DONNÉES SENSIBLES

1. Respecter les droits de la personne concernée avant de collecter ses données sensibles
2. Renforcer les politiques relatives à la sécurité des informations sensibles

CHAPITRE IX

DROITS DES PERSONNES CONCERNÉES

9.1 DROIT D'ACCÈS

1. Lorsque les données d'une personne concernée sont traitées dans le Système aux fins de l'application de la loi, le service chargé de l'application de la loi doit, dès que les circonstances l'y autorisent en toute sécurité, lui permettre d'accéder, directement ou indirectement, à ces données à sa demande, sous réserve du respect du cadre juridique applicable.
2. En ce qui concerne l'accès direct, la personne concernée peut déposer sa demande d'accès directement auprès du service chargé de l'application de la loi responsable des données. Celuici doit évaluer la demande, ainsi que les restrictions ou dérogations éventuelles qui peuvent être appliquées si cela est nécessaire aux fins de l'application de la loi, ou si cela est nécessaire pour protéger la personne concernée ou les droits et libertés de tiers, puis il doit répondre directement à la personne concernée.
3. En ce qui concerne l'accès indirect, la personne concernée doit s'adresser à l'autorité de protection des données, qui peut procéder à la demande pour son compte et mener des vérifications quant à la disponibilité de données et la licéité du traitement des données à caractère personnel de la personne concernée. L'autorité de protection des données peut ensuite répondre à la personne concernée en conséquence.
4. L'accès doit être direct, sous réserve du respect du cadre juridique applicable, si un pays participant au SIPAO ne dispose actuellement pas d'une autorité de protection des données fonctionnelle, et tant que cet organisme n'a pas été établi.
5. Le droit d'accès direct peut être restreint si un pays participant au SIPAO dispose d'une autorité de protection des données fonctionnelle, dont le cadre juridique autorise une personne concernée à exercer un droit d'accès indirect à ses données à caractère personnel par l'intermédiaire de cette autorité.
6. Lorsque cela est nécessaire et proportionné, le droit d'accès peut être exceptionnellement restreint ou exclu, en totalité ou en partie, conformément au cadre juridique applicable, pour :
   a. éviter d'entraver des recherches, des enquêtes ou des procédures officielles ou judiciaires ;
   b. éviter de nuire à la prévention, à la détection, aux enquêtes ou aux poursuites d'infractions pénales, ou à l'exécution de sanctions pénales ;
   c. protéger les droits et libertés de tiers ;
   d. protéger une enquête, des poursuites ou toute autre tâche importante d'application de la loi en cours ;

e. protéger les intérêts de l'État (comme la sécurité publique, la sécurité nationale, etc.) ;

7. Lorsque le droit d'accès est limité ou exclu, le service chargé de l'application de la loi concerné ou l'autorité de protection des données doit informer la personne concernée par écrit et sans délai des motifs du refus ou de la restriction. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'une des finalités énoncées au paragraphe 6 cidessus. Le service chargé de l'application de la loi doit informer la personne concernée de la possibilité d'introduire une réclamation auprès de l'autorité de protection des données ou de former un recours juridictionnel, le cas échéant.
8. Le droit d'accès doit, en principe, être exercé gratuitement. Des frais de gestion raisonnables peuvent être facturés au titre de la demande si la législation nationale le permet.
9. Le service chargé de l'application de la loi doit stipuler dans une politique ou un avis un délai raisonnable pour le traitement des demandes d'accès.

ÉTUDE DE CAS

SUR LE DROIT D'ACCÈS

Affaire Segerstedt-Wiberg et autres c. Suède, arrêt de la CEDH, 6 juin 2006, requête No 62332/00

Dans cette affaire, les requérants ont essayé d'avoir accès à leurs données à caractère personnel enregistrées dans les fichiers de la Sûreté suédoise. L'affaire concerne cinq personnes physiques : Mme Segerstedt-Wiberg, M. Nygren, M. Ehnebom, M. Frejd et M. Schmid. Le gouvernement suédois s'est appuyé sur la loi suédoise sur le secret de 1980 pour refuser de communiquer ces informations, arguant « [qu']il était impossible de divulguer d'autres informations sans compromettre le but des mesures prises ou prévues, ou nuire à des opérations futures ».

Mme Segerstedt-Wiberg a été une éminente députée du parti libéral suédois et a demandé l'accès aux dossiers de la police après la circulation d'informations préjudiciables à son encontre, notamment des rumeurs selon lesquelles elle était « peu fiable » par rapport à l'Union soviétique. La police a communiqué toutes les informations la concernant jusqu'en 1976, mais a restreint l'accès au reste du fichier en raison des menaces permanentes exercées contre elle. La Cour a admis que la conservation des informations en question poursuivait une finalité légitime (la défense de l'ordre ou la prévention d'infractions pénales) et n'avait pas de raison de douter des motifs du gouvernement de ne pas lui divulguer les informations à la lumière des menaces de sécurité dirigées contre elle (par exemple, menace d'attentat à la bombe en 1990).

M. Nygren est un journaliste qui a rédigé un certain nombre d'articles sur le nazisme et sur la Sûreté suédoise. Il a eu accès à deux pages de son dossier, mais n'a pu consulter le reste. La Cour a déclaré que la nature et l'ancienneté des informations ne justifiaient pas d'en maintenir la conservation au titre de la protection de la sécurité nationale.

M. Ehnebom était un membre du KPML, un parti marxiste-léniniste suédois. Il a eu accès à 30 pages de son dossier et, selon lui, les informations qui y étaient contenues ont été la cause de son licenciement. M. Frejd a aussi été membre du KPML et était bien connu dans les milieux sportifs suédois. Il a été autorisé à consulter des parties de son dossier portant sur sa participation au KPML, notamment sa tentative de se faire élire en tant que membre du parti.

Toutefois, il n'a pu consulter l'intégralité de son dossier. Pour ces deux requérants, la Cour a reconnu qu'ils étaient tous deux membres d'une organisation défendant l'opposition armée et la domination d'un groupe sur un autre, mais que cela constituait le seul élément de preuve utilisé par le gouvernement suédois pour justifier la conservation des données à caractère personnel.

M. Schmid a été député au Parlement européen et a fait partie du parti de gauche suédois. Il a eu accès à certaines archives concernant sa participation à des campagnes pour le désarmement nucléaire et son appartenance à des groupes sociaux-démocrates. La Cour n'a trouvé aucun motif permettant d'asseoir la pertinence de la conservation et de la restriction d'accès à son dossier au titre de l'intérêt de la sécurité nationale de la Suède et a jugé que la conservation de ces informations était disproportionnée au regard des buts légitimes de la loi.

9.2 DROIT DE RECTIFICATION OU D'EFFACEMENT

1. Les personnes concernées peuvent demander, directement ou indirectement, au service chargé de l'application de la loi de rectifier ou d'effacer des données à caractère personnel inexactes les concernant qui sont enregistrées dans le Système, conformément au cadre juridique applicable du pays participant au SIPAO en question. Les personnes concernées peuvent aussi demander que les données à caractère personnel incomplètes soient complétées.
2. En ce qui concerne l'exercice direct de ce droit, la personne concernée peut déposer sa demande de rectification ou d'effacement directement auprès du service chargé de l'application de la loi responsable des données. Celuici doit évaluer la demande, ainsi que les restrictions ou dérogations éventuelles qui peuvent être appliquées si cela est nécessaire aux fins de l'application de la loi, ou si cela est nécessaire pour protéger la personne concernée ou les droits et libertés de tiers, puis il doit répondre directement à la personne concernée.

3. En ce qui concerne l'exercice indirect de ce droit, la personne concernée doit s'adresser à l'autorité de protection des données qui peut procéder à la demande de rectification ou d'effacement pour son compte et mener des vérifications quant à la disponibilité et la licéité du traitement des données à caractère personnel de la personne concernée. L'autorité de protection des données peut ensuite répondre à la personne concernée en conséquence.
4. Le droit de rectification ou d'effacement doit être directement exercé auprès du service chargé de l'application de la loi concerné, sous réserve du respect du cadre juridique applicable, si un pays participant au SIPAO ne dispose pas d'une autorité de protection des données fonctionnelle.
5. Le droit à la demande directe de rectification ou d'effacement peut être restreint si un pays participant au SIPAO dispose d'une autorité de protection des données fonctionnelle, dont le cadre juridique autorise une personne concernée à exercer son droit de rectification ou d'effacement indirectement par l'intermédiaire de cette autorité.
6. Au lieu de procéder à l'effacement, les services chargés de l'application de la loi doivent restreindre le traitement lorsque :
   a. l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non ; ou
   b. les données à caractère personnel doivent être conservées à des fins probatoires.
7. Le service chargé de l'application de la loi ou l'autorité de protection des données, le cas échéant, doit informer la personne concernée par écrit de tout refus de rectifier ou d'effacer des données à caractère personnel ou d'en restreindre le traitement, ainsi que des motifs du refus.
8. Conformément à la législation en vigueur, le service chargé de l'application de la loi concerné peut limiter, en tout ou en partie, son obligation de fournir ces informations, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne concernée ainsi que des lois applicables pour :
   a. éviter d'entraver des recherches, des enquêtes ou des procédures officielles ou judiciaires ;
   b. éviter de nuire à la prévention, à la détection, aux enquêtes ou aux poursuites d'infractions pénales, ou à l'exécution de sanctions pénales ;
   c. protéger les droits et libertés de tiers ;
   d. protéger une enquête, des poursuites ou toute autre tâche importante d'application de la loi en cours ;
   e. protéger les intérêts de l'État (comme la sécurité publique et la sécurité nationale ;
9. Lorsqu'un service chargé de l'application de la loi a rectifié, effacé ou restreint le traitement de données à caractère personnel, il doit en avertir tous les destinataires auxquels il a transféré ces données et leur demander de faire de même.

ÉTUDE DE CAS

SUR LE DROIT DE RECTIFICATION DES DONNÉES À CARACTÈRE PERSONNEL

Affaire Khelili c. Suisse, arrêt de la CEDH, 18 octobre 2011, requête No 16188/07

En 1993, la police de Genève a enregistré des informations sur Mme Khelili avec la mention « prostituée » dans sa base de données. La loi suisse autorisait la police à conserver les enregistrements tant que les données étaient nécessaires pour lui permettre de remplir ses missions (à savoir répression des infractions et prévention de la criminalité). En 2001, 2002 et 2003, des plaintes pénales indépendantes ont été déposées contre Mme Khelili pour insultes et menaces. À cette époque, elle a découvert que la police conservait la mention « prostituée » dans son dossier. En 2006, elle a demandé que cette mention soit supprimée de son dossier et a été informée, par le chef de la police, que cela avait été fait. Toutefois, même si le dossier de 1993 a été modifié, la mention « prostituée » a été conservée en lien avec les plaintes de 2001, 2002 et 2003.

La Cour a convenu que l'inscription de la mention « prostituée » dans le dossier de police de Mme Khelili constituait une ingérence, mais qu'elle avait un fondement juridique ayant pour but la défense de l'ordre, la prévention des infractions pénales et la protection des droits d'autrui. La mention « prostituée » comme profession a été supprimée de la base de données informatisée de la police, mais n'a pas été corrigée dans les procédures pénales relatives aux autres plaintes déposées contre elle et pouvait nuire à sa réputation, tant dans la sphère privée que dans la sphère publique. La Cour a d'abord tenu compte du fait que l'allégation de prostitution paraissait vague et générale et que le lien entre le dossier de 1993 et les plaintes de 2001, 2002 et 2003 n'étaient pas suffisamment étroits. La Cour a aussi noté le fait que la police avait supprimé la mention « prostituée » d'une partie du dossier de Mme Khelili, mais pas de la totalité, tout en l'informant avoir expurgé son dossier pour supprimer cette mention. De ce fait, la police conservait une donnée erronée la concernant et le maintien de la mention « prostituée » dans son dossier n'était ni justifié, ni nécessaire dans une société démocratique.

BONNES PRATIQUES

DROITS DES PERSONNES CONCERNÉES

1. Respecter l'exercice du droit d'accès des personnes concernées

2. Respecter l'exercice du droit de rectification et d'effacement des données à caractère personnel inexactes enregistrées dans le Système

CHAPITRE X

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

10.1 ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

1. Les services chargés de l'application de la loi doivent remplir et documenter une analyse d'impact relative à la protection des données afin de consigner les risques identifiés et les mesures qui ont été mises en œuvre pour les gérer.
2. Lorsque cela est nécessaire, cette analyse d'impact relative à la protection des données doit être réalisée avant la mise en œuvre du Système, puis à intervalles réguliers.
3. L'analyse d'impact doit identifier et tenir compte :
   a. des informations permettant de savoir quelles données doivent être traitées ou sont traitées ;
   b. des personnes ou de la catégorie de personnes dont les données seront ou sont traitées ;
   c. du type de traitement, avec un calendrier de la collecte à l'effacement des données ;
   d. des risques associés au traitement réalisé ;
   e. des mesures prises pour gérer les risques identifiés ;
   f. des régimes/obligations légaux qui vont s'appliquer, le cas échéant ;
   g. des orientations fournies par l'autorité de protection des données ;
   h. de tous les risques résiduels, ou des mesures qui ne peuvent être gérées ou mises en œuvre, avec la justification et l'acceptation de ces risques.
4. Aux fins de cette étude d'impact, les services chargés de l'application de la loi doivent élaborer une approche fondée sur le risque et l'appliquer au programme SIPAO en s'appuyant sur les bonnes pratiques ainsi que sur les risques liés à la conformité juridique et réglementaire. À cet effet, ils doivent :
   a. comprendre les risques liés à la protection des données au sein du SIPAO, ses objectifs organisationnels globaux, sa culture, son langage et ses opérations ;
   b. identifier dans quels domaines des données à caractère personnel sont susceptibles d'être collectées, traitées ou utilisées au sein du SIPAO ; et
   c. déterminer, sur la base des risques identifiés en matière de protection des données, quelles priorités y afférentes doivent être alignées sur les objectifs globaux.

BONNES PRATIQUES

ANALYSE D'IMPACT

Procéder à une analyse d'impact relative à la protection des données avant la mise en œuvre du Système, puis à intervalles réguliers

Vérifier si le traitement des données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées

CHAPITRE XI

DÉROGATIONS

11.1 DÉROGATIONS AU TRAITEMENT DES DONNÉES CONFORMÉMENT AU PRÉSENT GUIDE

1. Les dérogations au traitement des données conformément au présent Guide ne doivent être invoquées que dans la mesure où :
   a. elles sont expressément prévues par la loi ;
   b. elles constituent une mesure nécessaire et proportionnée pour la protection de la sécurité nationale, la défense, la sécurité publique, d'intérêts économiques et financiers importants, l'impartialité et l'indépendance du pouvoir judiciaire, la prévention, les enquêtes et les poursuites d'infractions pénales, l'exécution de sanctions pénales, la protection des buts d'intérêt général essentiels ou les droits et libertés fondamentaux de tiers.
2. Si une dérogation définie par le droit national assortie de garanties spécifiques est invoquée par les services chargés de l'application de la loi, elle doit être appliquée pour des buts légitimes et uniquement dans la mesure nécessaire et proportionnée en vue de réaliser le but pour lequel elle est appliquée. L'invocation des dérogations par les services chargés de l'application de la loi doit être limitée aux affaires où leur noninvocation risquerait de nuire à la finalité en matière d'application de la loi fondant le traitement des données.

CHAPITRE XII

CONCLUSION

Le présent Guide n'a pas vocation à être un texte législatif ou réglementaire. Il se veut un document de référence qui guidera les services chargés de l'application de la loi dans l'application des principes juridiques de la protection des données, ou un instrument d'autorégulation lorsqu'il n'existe pas de lois relatives à la protection des données. Correctement mis en œuvre, il permettra aux pays participant au SIPAO d'adopter des bonnes pratiques qui faciliteront le partage des informations et optimiseront l'utilisation du Système. Il peut aussi guider la mise en œuvre de la protection des données audelà du Système dans le cadre des opérations globales d'un service chargé de l'application de la loi.

PRINCIPAUX POINTS À RETENIR

INTRODUCTION

Les chefs d'État et de gouvernement des États membres de la Communauté économique des États de l'Afrique de l'Ouest (« CEDEAO ») ont signé l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO (« l'Acte ») le 16 février 2010.

L'Acte :

- établit les principes fondamentaux applicables au traitement des données à caractère personnel dans le système d'information policière pour l'Afrique de l'Ouest (« SIPAO ») ; et
- enjoint les États membres d'adopter des lois relatives à la protection des données et de mettre en place une autorité de protection des données.

CHAPITRE I – TERMES ET EXPRESSIONS

Le premier chapitre présente les termes et expressions utilisés dans le Guide.
Il identifie :

- qui doit se conformer à l'Acte ? Les responsables du traitement et les sous-traitants
- qui reçoit des données à caractère personnel ? Les destinataires
- qui fait l'objet des opérations de traitement des données à caractère personnel ? Les personnes concernées
- quel type d'information est réglementé au titre de l'Acte ? Les données à caractère personnel.

CHAPITRE II – PRINCIPES ET FINALITÉ

Le deuxième chapitre présente les principes généraux de la protection des données à caractère personnel et les finalités légitimes en matière d'application de la loi qui en justifient le traitement.

2.1 – Principes applicables en matière de protection des données à caractère personnel

Les principes de la protection incluent les principes suivants :

› 2.2 – Finalité du traitement des données dans le Système

Les services chargés de l'application de la loi doivent être sensibilisés aux situations pouvant les amener à traiter des données dans le SIPAO. Ces finalités comprennent :

- la prévention, les enquêtes, la détection ou les poursuites des infractions ;
- l'exécution des sanctions ;
- le maintien de l'ordre public ;
- la protection contre les menaces à la sécurité publique et la prévention de ces dernières ;
- toute obligation ou responsabilité légale qui leur incombent.

CHAPITRE III – RÉGIME DE PROTECTION DES DONNÉES ET GOUVERNANCE

Le troisième chapitre aborde les autorités de protection des données, la sensibilisation et la formation à la protection des données et la conformité générale.

› 3.1 – Contrôle et notification

Tous les pays participant au SIPAO doivent mettre en place une autorité de protection des données indépendante responsable de la supervision de toutes les opérations de traitement des données.

› 3.2 – Officier délégué à la protection des données et sensibilisation et formation à la protection des données

Les services chargés de l'application de la loi doivent désigner un officier délégué à la protection des données chargé de :

- les conseiller quant aux obligations légales qui leur incombent ;
- contrôler la conformité ;
- fournir des conseils sur les analyses d'impact relatives à la protection des données ;
- assurer la liaison avec les autorités de protection des données ; et
- mettre en place des programmes de formation continue adaptés destinés aux utilisateurs du SIPAO.

› 3.3 – Respect de la législation relative à la protection des données et gouvernance

Les services chargés de l'application de la loi doivent intégrer la protection des données à leur structure de gouvernance en impliquant les parties prenantes clés dans le cadre de protection des données du SIPAO.

CHAPITRE IV – COLLECTE ET PARTAGE DES DONNÉES À CARACTÈRE PERSONNEL

Le quatrième chapitre présente les bonnes pratiques en matière de collecte et de partage des données à caractère personnel.

› 4.1 – Collecte des données à caractère personnel.

De manière générale, la collecte des données à caractère personnel doit être limitée à ce qui est nécessaire et proportionné aux finalités en matière d'application de la loi pour lesquelles elles sont collectées.

4.2 – Partage ou transmission des données à d'autres organismes publics.

Une fois les données à caractère personnel collectées, les services chargés de l'application de la loi peuvent les partager avec d'autres organismes publics (n'étant pas des services chargés de l'application de la loi) si ce partage est prévu par la loi et si les données sont demandées par le destinataire afin de lui permettre de mener une tâche légale.

4.3 – Partage ou transmission des données à des organismes privés ou au grand public. organismes publics.

Une fois les données à caractère personnel collectées, les services chargés de l'application de la loi peuvent les partager avec des organismes privés si ce partage est effectué pour réaliser les finalités en matière d'application de la loi ; pour prévenir un risque grave et imminent pour la sécurité publique ; dans l'intérêt des personnes concernées ; ou pour des raisons humanitaires. Une fois les données à caractère personnel collectées, les services chargés de l'application de la loi peuvent les partager avec le grand public si cela lui permet de l'alerter ; de solliciter son aide ; ou pour réaliser toute autre finalité en matière d'application de la loi.

4.4 – Partage ou transmission des données au niveau international.

Une fois les données à caractère personnel collectées, les services chargés de l'application de la loi peuvent les partager avec des services chargés de l'application de la loi internationaux ou des organisations internationales si : a) le service destinataire réalise une fonction qui lui est conférée par la loi à des fins d'application de la loi ; b) le partage des données est nécessaire pour qu'il réalise ses obligations en matière d'application de la loi ; c) le service qui partage les informations s'assure que le service destinataire garantit un niveau de protection adéquat en matière de sécurité des informations dans le cadre du traitement desdites données.

CHAPITRE V – QUALITÉ, CONFIDENTIALITÉ ET SÉCURITÉ DES DONNÉES

Le cinquième chapitre aborde la question de la qualité des données et les mesures que les services chargés de l'application de la loi doivent mettre en œuvre pour préserver la confidentialité et la sécurité des données à caractère personnel.

› 5.1 – Qualité des données

Les services chargés de l'application de la loi ne doivent pas partager de données à caractère personnel qui sont inexactes, incomplètes ou obsolètes. Si des données à caractère personnel inexactes sont partagées, les services chargés de l'application de la loi doivent en avertir sans délai le destinataire et prendre les mesures nécessaires pour les rectifier, les effacer ou en restreindre le traitement.

› 5.2 – Confidentialité et sécurité

Les services chargés de l'application de la loi doivent prendre des mesures adaptées, raisonnables et techniques pour sécuriser le SIPAO contre les risques d'accès, de destruction, de perte, d'utilisation, de modification ou de divulgation accidentels ou non autorisés des données à caractère personnel.

CHAPITRE VI – VIOLATIONS DE DONNÉES

Le sixième chapitre décrit les mesures adaptées que les services chargés de l'application de la loi doivent déployer en cas de violation de données.

VIOLATION DE DONNÉES

AUTORITÉ DE PROTECTION DES DONNÉES

6.1 – NOTIFICATION DES VIOLATIONS DE DONNÉES.
Les services chargés de l'application de la loi doivent répertorier et signaler sans délai les violations de données à l'autorité de protection des données concernée, de préférence dans les 72 heures à compter de la violation initiale.

PERSONNES CONCERNÉES

6.2 – NOTIFICATION DES VIOLATIONS DE DONNÉES AUX PERSONNES CONCERNÉES.
Les services chargés de l'application de la loi doivent avertir sans délai les personnes concernées de toute violation de données si celle-ci est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.de la violation initiale.

CHAPITRE VII – TRAITEMENT DES REGISTRES ET CONSERVATION DES DONNÉES

Le septième chapitre présente les bonnes pratiques en ce qui concerne le traitement des registres et la conservation des données.

› 7.1 – Registres des activités de traitement des données.

Les services chargés de l'application de la loi doivent conserver des registres de toutes les activités de traitement des données.

› 7.2 – Journaux.

Les services chargés de l'application de la loi doivent conserver des journaux sur les opérations de traitement des données suivantes : a) collecte ; b) modification ; c) accès/consultation ; d) communication, dont les transferts ; e) interconnexion ; f) effacement.

› 7.3 – Conservation des données.

Les services chargés de l'application de la loi ne doivent conserver les données que pour une période adéquate.

CHAPITRE VIII – TRAITEMENT DES DONNÉES SENSIBLES

Le huitième chapitre explique que les données sensibles (« données à caractère personnel qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'orientation sexuelle, ainsi que les données génétiques ou plus généralement les données sur l'état de santé d'une personne physique » [Ch. 8.1, para. 1]) ne doivent être traitées dans le SIPAO qu'en cas de nécessité absolue.

CHAPITRE IX – DROITS DES PERSONNES CONCERNÉES

Le neuvième chapitre présente les droits d'accès, de rectification ou d'effacement des personnes concernées.

› 9.1 – Droit d'accès et 9.2 – Droit de rectification ou d'effacement.

9.1 – DROIT D'ACCÈS
Le droit d'accès donne la capacité à une personne concernée d'accéder, directement ou indirectement, aux données la concernant traitées dans le SIPAO.

9.2 – DROIT DE RECTIFICATION OU D'EFFACEMENT
Le droit de rectification ou d'effacement donne la capacité à une personne concernée de demander aux services chargés de l'application de la loi de rectifier ou d'effacer des données à caractère personnel inexactes la concernant enregistrées dans le SIPAO.

CHAPITRE X – ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Le dixième chapitre aborde les analyses d'impact relatives à la protection des données, un mécanisme qui peut aider les services chargés de l'application de la loi à évaluer et à consigner les risques encourus lors de la mise en œuvre du SIPAO. Une analyse d'impact relative à la protection des données adéquate prouvera que les services chargés de l'application de la loi ont tenu compte des risques afférents au traitement prévu ainsi que de leurs obligations plus larges en matière de protection des données.

CHAPITRE XI – DÉROGATIONS

Le onzième chapitre recense les situations, rares, dans lesquelles les données peuvent ne pas être traitées conformément au présent Guide.

CHAPITRE XII – CONCLUSION

Enfin, le douzième chapitre fait la synthèse de l'objectif global du présent Guide, qui est de permettre aux pays participant au SIPAO d'adopter des pratiques de traitement des données légales qui facilitent le partage des informations et optimisent l'utilisation du SIPAO.

INTERPOL

INTERPOL BUREAU RÉGIONAL ABIDJAN
ANNEXE
RUE E70, À PROXIMITÉ DE L'ÉGLISE
BON PASTEUR
RIVIERA 3 EECI, LOT 1199 ILOT 125
ABIDJAN
CÔTE D'IVOIRE

WWW.INTERPOL.INT

@INTERPOL_HQ WWW.INTERPOL.INT INTERPOLHQ