COMMISSION DE PROTECTION DES DONNEES PERSONNELLES DELIBERATION N° 2014–014/CDP DU 3 AVRIL 2014 PORTANT SUR LES MESURES DE SECURITE APPLICABLE AUX TRAITEMENTS DES DONNEES A CARACTERE PERSONNEL

LA COMMISSION DE PROTECTION DES DONNEES PERSONNELLES DU SENEGAL (CDP), réunie en session plénière le 3 avril 2014 sous la présidence du **Dr Mouhamadou LO**, Président ;

Vu la loi n° 2008-12 du 25 janvier 2008 sur les données à caractère personnel (LDP) en particulier en ses articles 39, 49 et 71 et suivants ;

Vu le décret n°2008-721 du 30 juin 2008 portant application de la loi n° 2008-12 du 25 janvier 2008 précitée en particulier en son article 65 ;

Vu la délibération n° 2014-001 du 31 janvier 202014 portant règlement intérieur de la Commission de protection des données personnelles ;

Vu le procès-verbal de la session plénière du 3 avril 2014 de la Commission de protection des données personnelles ;

RECOMMANDE, APRES DELIBERATION, LES PRESENTES MESURES DE SECURITE.

I –OBJET DE LA DELIBERATION

La présente délibération a pour objet de rappeler les principes relatifs aux mesures de sécurité applicables aux traitements de données personnelles conformément aux dispositions des articles 39, 49, 71 et suivants de la loi 2008-12 portant sur la protection des données à caractère personnel.

A cet effet, la CDP rappelle que le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Par ailleurs, en application de l'article 65 du décret n°2008-721 du 30 juin 2008 sus visé, le responsable du traitement des données à caractère personnel est tenu de prendre des mesures de sécurité pour protéger les systèmes et les réseaux informatiques notamment contre les risques de destruction accidentelle ou non autorisée des données collectées, d'erreurs techniques, de falsification, de vol ou d'utilisation illicite desdites données.

II - PERSONNES CONCERNEES

La présente délibération concerne tous les responsables de traitement de données à caractère personnel des sénégalais, y compris leurs sous-traitants. En application de l'article 4-5 de la loi du 25 janvier 2008 susmentionnée, le responsable du traitement est la « *personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités* ».

III - MESURES DE SECURITE LORS DE LA COLLECTE, DU TRAITEMENT ET DU STOCKAGE

En application de l'article 71 de la loi du 25 janvier 2008, le responsable d'un traitement de données à caractère personnel doit, pour assurer la protection d'un système d'information, entreprendre la démarche suivante ou équivalente :

- déterminer et identifier de la façon la plus précise qui soit, les risques et les menaces pouvant porter atteinte à l'intégrité, à la confidentialité et à la disponibilité des données ;
- mettre en œuvre des mesures de sécurité appropriées contre ces risques et menaces identifiées.

Ces mesures devront couvrir au moins les points ci-dessous :

3.1 IDENTIFICATION ET AUTHENTIFICATION

Le responsable d'un traitement de données à caractère personnel doit :

- mettre en place un système d'identification et d'authentification (Login personnel, mot de passe, badge d'accès aux salles des serveurs, etc.) pour toutes les personnes habilités à accéder directement ou indirectement aux données ;
- mettre en œuvre un système de traçabilité des actions des utilisateurs.

3.2 CONFIDENTIALITE ET INTEGRITE DES DONNEES

Le responsable d'un traitement de données à caractère personnel doit :

- utiliser des mécanismes et des procédures garantissant la confidentialité et l'intégrité des données par un système d'enregistrement quotidien de toutes les actions et des accès aux données ;
- prévoir des moyens de chiffrement en cas de stockage pour empêcher que des données puissent être lues, copiées, modifiées, détruites ou déplacées par une personne non autorisée.

- stocker les supports de sauvegarde dans un endroit distant sûr et sécurisé.

3.3 - Mesures de sécurité organisationnelle

Le responsable d'un traitement de données à caractère personnel doit, en application de l'article 71 de la loi du 25 janvier 2008, prendre les mesures de sécurité organisationnelles ci-après consistant à « *empêcher toute personne non autorisée d'accéder aux locaux et aux équipements utilisés pour le traitement des données* ».

Exemples de mesures :

- Prévoir des dispositifs d'authentification avant d'accéder aux locaux et équipements ;
- Exiger le port d'un moyen d'identification visible ;
- Installer des alarmes anti-intrusion ;
- Exiger à toute personne autorisée à accéder et à manipuler les données traitées à signer une clause de confidentialité.
-

IV. LES MESURES DE SECURITE EN CAS DE TRANSMISSION, DE TRANSFERT, DE SAUVEGARDE ET DE CONSERVATION DES DONNEES

4.1 - En cas de transmission de données

Le responsable d'un traitement de données à caractère personnel doit prendre des mesures de sécurité consistant notamment à « *garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données à caractère personnel peuvent être transmises* ».

Exemples de mesures :

- S'assurer de l'identité du destinataire des données et de l'accomplissement des formalités de déclaration auprès de l'autorité de protection des données personnelles.
- Chiffrer les données avant leur envoi vers le destinataire.
- Transmettre le mot de passe (secret) lors d'un envoi distinct et via un canal différent.

4.2 – En cas de transfert de données

Lorsque le responsable d'un traitement envisage de transférer des données vers l'étranger, soit sur des supports physiques ou sur un réseau, il doit empêcher que « *les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée* ».

Exemples de mesures :

- Prévoir des moyens de chiffrement des supports physiques.

- Utiliser un protocole garantissant la confidentialité et l'authentification des communications.

4.3 - Pour la sauvegarde de données

La sauvegarde des données personnelles requiert des mesures de sécurité en vue de préserver leur intégrité et faciliter leur récupération ultérieure.

Exemples de mesures :

- Sauvegarder les données par la constitution de copies de sécurité.
- Effectuer des sauvegardes fréquentes pour respecter le principe de pérennité des données.

4.4 - Pour la conservation des données

En application de l'article 72 de la loi du 25 janvier 2008, les données à caractère personnel « *ne peuvent être conservées au-delà de la durée nécessaire qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques* ».

Exemples de mesures :

- Respecter les durées légales de conservation des données ou les décisions de la CDP en la matière.
- Vérifier que le traitement permet de détecter la date prévue pour la fin de la durée de conservation des données.
- Vérifier que le traitement permet de supprimer les données dès la fin de la durée de conservation.

V. LES SOUS-TRAITANTS DES RESPONSABLES DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Tout sous-traitant doit veiller au respect des mesures de sécurité mentionnée à l'article 71 de la loi sur les données personnelles.

Le contrat ou l'acte juridique consigné par écrit et qui lie le responsable du traitement au sous-traitant, tel que prévu à l'article 39 de la loi sur les données à caractère personnel, doit comporter une clause de confidentialité sur les données traitées et disposer que le sous-traitant ne doit recevoir des instructions que du responsable du traitement.

Exemples de mesures :

- Prévoir une clause de confidentialité dans les contrats.
- Vérifier l'effectivité des garanties contractuelles (audits de sécurité, visites…).

- Faire signer un engagement de confidentialité à tout autre intervenant dans le traitement des données.
- Préciser clairement le rôle exact du sous-traitant et des autres intervenants.

VI. LES SANCTIONS

En application des articles 30 de la loi sur les données à caractère personnel, 67 et suivants de son décret d'application et 431-21 du Code pénal, des sanctions administratives, pécuniaires et pénales peuvent être prononcées, à l'égard de tout responsable d'un traitement n'ayant pas respecté ses obligations, soit par la CDP ou par les juridictions compétentes.