COMMISSION DE PROTECTION DES DONNÉES PERSONNELLES

DELIBERATION **N°2017-00306/CDP DU 20 OCTOBRE 2017 METTANT EN DEMEURE LA CBAO ATTIJARIWAFA BANK** POUR MANQUEMENT AUX DISPOSITIONS DE LA LEGISLATION SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL.

LA COMMISSION DE PROTECTION DES DONNEES PERSONNELLES DU SENEGAL (CDP), réunie en session plénière le 20 octobre 2017 sous la présidence de Madame Awa NDIAYE, Présidente ;

Vu la Constitution ;

Vu la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel ;

Vu la loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques ;

Vu le décret n° 2008-721 du 30 juin 2008 portant application de la loi n° 2008-12 du 25 janvier 2008 ;

Vu la délibération modificative N°2016-00230/CDP du 26 aout 2016 portant règlement intérieur de la Commission de protection des données personnelles (CDP);

Vu la délibération de portée générale n°2014-14/CDP du 03 avril 2014 portant sur les mesures de sécurité applicable aux traitements de données à caractère personnel ;

Vu la lettre n°000898/CDP du 11 novembre 2014 portant relance en vue de la déclaration des fichiers de données personnelles

Vu la lettre N° 669/14 FDN / BDN du 09 décembre 2014 portant bordereau d'envoi de déclaration de fichiers de données personnelles (fichier du personnel, système de vidéosurveillance, badges, données de la clientèle) et demande d'autorisation des données envoyées à un pays tiers ;

Vu le procès-verbal n°2017- 0011C/CDP du 17 aout 2017 de la mission de contrôle sur site auprès de la CBAO Attijariwafa BANK.

Vu le procès-verbal de la session plénière du 20 octobre 2017 de la Commission de protection des données personnelles ;

EMET, APRES DELIBERATION, LA DECISION SUIVANTE :

1. FAITS ET PROCEDURE :

La CBAO Groupe Attijariwafa bank est la filiale du groupe financier marocain Attijariwafa Bank.

Suite à deux courriers de relance d'appel à déclaration des traitements de données à caractère personnel, la CBAO Attijariwafa BANK a transmis à la CDP le 09 décembre 2014, par bordereau d'envoi, des déclarations et une demande d'autorisation portant sur :

- le fichier du personnel ;
- le système de vidéosurveillance ;
- les badges ;
- les données de la clientèle ;
- le transfert de données vers un pays tiers.

Le 09 janvier 2015, la Session plénière de la Commission de protection des Données Personnelles par délibération a délivré des récépissés pour les traitements susvisés, et accordé une autorisation à poursuivre le traitement portant transfert de données vers un pays tiers.

Conformément au programme annuel des missions de contrôle sur site, par décision n°2017-11C/CDP du 10 aout 2017, la Session plénière a demandé aux Commissaires et agents habilités de procéder à une mission de contrôle auprès de la CBAO Attijariwafa BANK.

La délégation de la CDP, chargée de la mission, s'est attachée à vérifier la conformité des traitements relatifs à la gestion administrative du personnel et à la gestion de la clientèle.

2. MANQUEMENTS CONSTATES AU REGARD DE LA LOI N°2008-12 DU 25 JANVIER PORTANT SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

A. LE TRAITEMENT RELATIF A LA GESTION ADMINISTRATIVE DU PERSONNEL

- **Sur le manquement à l'obligation de conserver les données pour une durée définie :**

La CBAO Attijariwafa BANK collecte les données de ses salariés à des fins d'identification lors d'un traitement administratif.

Il ressort du procès-verbal de la mission de contrôle que « *la CBAO reçoit de façon spontanée des demandes de stages ou d'emploi par mail ou de façon physique. Un classement est fait par profil, par métier.*

Les dossiers des candidats non-présélectionnés sont conservés pendant trois (03) ans, puis archivés ;

Si un dossier de candidature aboutit à un entretien, davantage de documents sont demandés aux candidats, et ces données sont conservées, quel que soit l'issu de l'entretien.

La CBAO reçoit plus de 60 ***demandes par jours****, et il n'existe pas de procédures formelles de traitement des données personnelles des demandeurs d'emploi* ».

En application des dispositions de l'article 35-3 de la loi n°2008-12 précitée, « *les données doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées* ».

Au regard du procès- verbal de contrôle, il apparait que la durée de conservation des données des demandeurs d'emploi sélectionnés à un entretien n'est pas définie. Cela constitue un manquement à l'obligation de définir une durée de conservation des données.

B. LE TRAITEMENT RELATIF A LA GESTION DE LA CLIENTELE

- **Sur le manquement à l'obligation de sécurité et de confidentialité :**

a) L'accès aux données par des personnes non habilitées

Conformément à l'article 71-1 de la loi n°2008-12 précitée « *le responsable de traitement doit prendre, en particulier, toute mesure visant à garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données à caractère personnel relevant de leur compétence* ».

Il ressort du procès-verbal de la mission de contrôle que la CBAO a adopté une politique de sécurité globale. Chaque utilisateur (salarié ou stagiaire) doit, en principe, disposer d'un compte Windows qui lui permet d'accéder au système d'information de la banque. La communication des identifiants (login, mot de passe) est formellement interdite aux agents.

Toutefois, avons constaté au jour du contrôle qu'une stagiaire utilise les identifiants d'un agent permissionnaire depuis un mois. Avons aussi constaté, qu'avec le voisinage réseau, il est possible d'accéder à un certain nombre de fichiers des postes de travail du même sous-réseau. Les manipulations effectuées lors du contrôle ont permis d'accéder, à partir d'un ordinateur distant, à des documents confidentiels, notamment ceux relatifs à la situation des comptes clients, et à des informations à caractère privé, dont une demande d'explication servie à un salarié.

L'accès à des informations confidentielles, par une personne non habilitée, constitue un manquement à l'obligation de sécurité et de confidentialité.

b) Le recours à Windows XP

Le Responsable Réseau et Télécom a informé la délégation de la CDP que « *quatre (04) postes sont encore sous Windows XP, qu'un processus de migration est en cours pour remplacer les systèmes d'exploitation desdits postes* ».

Pour rappel, Microsoft, dans un article, informe que « *les PC qui exécutent Windows XP après le 8 avril 2014 ne sont pas considérés comme sûrs* ».

Une faille non comblée sur le système Windows XP (devenu obsolète) pourrait rendre vulnérable aux cyberattaques le système d'information de la CBAO.

En conséquence, la Session plénière, en application des dispositions de l'article 29-1 de la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel et des articles 25, 26 et 59 du règlement intérieur de la Commission, décide :

- **de mettre en demeure CBAO Attijariwafa BANK, dans un délai d'un (01) mois à compter de la notification de la présente décision et sous réserve des mesures à adopter, notamment de :**
  - **respecter les obligations de sécurité telles que définie à l'article 71-1 ;**
  - **définir des procédures formelles de conservation des dossiers des demandeurs d'emploi et de stages ;**

- de finaliser le processus de migration des postes sous Windows XP vers un Système d'Exploitation supporté par l'éditeur ;

- de publier ladite mise en demeure ;
- de demander à la CBAO Attijariwafa BANK de justifier auprès de la CDP que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.

À l'issue de ce délai, si la CBAO Attijariwafa BANK s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la CBAO ne s'est pas conformée à la présente mise en demeure, la Session plénière va demander au Comité de sanction de prononcer, après procédure contradictoire, une sanction pécuniaire conformément à l'article 30-2 de la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel.