POLITIQUE DE GESTION DES DONNEES PERSONNELLES DU GROUPE ALKALINE RGPD

1. OBJET

La politique de gestion des données personnelles (ci-après dénommée « la politique ») a pour objet de mettre en conformité les processus traitant des données personnelles au sein du groupe ALKALINE (ci-après « l'entreprise ») avec les dispositions européennes sur la protection des données personnelles (Règlement UE 2016/679 ci-après « RGPD »).

2. CHAMPS D'APPLICATION

- Les sociétés détenues majoritairement par l'entreprise,
- Tout processus de traitement de données personnelles, y compris si ce traitement est réalisé par un tiers (sous-traitant).

3. DEFINITIONS

Données personnelles : Toute information se rapportant à une personne physique identifiée ou identifiable, que ce soit directement (exemple : nom, prénom) ou indirectement (exemple : image, numéro de téléphone), qu'elle soit conservée sous format informatique ou papier. Les données concernant les sociétés personnes morales ne sont pas concernées.

4. ACTEURS DE LA DEMARCHE

Délégué à la protection des données (« DPD ») : Le DPD est le garant du respect par l'entreprise des règles de protection des données. Il réalise les évaluations de risque et anime le groupe de travail RGPD. Il rend compte au Management Committee de l'entreprise.

Le groupe de travail RGPD : Il suit les plans d'action, assure la communication sur le RGPD et la sensibilisation des équipes, définit des mesures pour réduire les risques au sein de l'entreprise.

Service Informatique : Le service informatique est responsable de l'exploitation et de la sécurité des systèmes et données informatiques. Il joue un rôle essentiel pour assurer la sécurité des données personnelles conservées sous format informatique, notamment au travers de solutions matérielles ou logicielles et de la formation des utilisateurs. Il participe aux évaluations de risques avec le DPD.

Responsables de traitement : Le responsable de traitement est la personne physique qui organise la collecte et le traitement de données.

Sous-traitants : Les sous-traitants effectuent des collectes et traitements de données pour le compte de l'entreprise. Ils doivent également respecter les règles de protection des données personnelles qui leur sont confiées ou auxquelles ils accèdent.

La CNIL : La CNIL est l'organisme chargé pour les activités basées en France de contrôler le respect du RGPD. Elle peut intervenir comme conseil en amont. Elle a le pouvoir de sanction.

Les salariés et managers : Sans en avoir nécessairement conscience, toute personne dans l'entreprise est susceptible de traiter des données à caractère personnel.

Le Management Committee : Le Management Committee (Comité de Direction) supervise les activités du DPD, alloue les moyens nécessaires à sa mission et définit ses objectifs annuellement.

5. OBJECTIFS POURSUIVIS PAR L'ENTREPRISE

5.1 Tenir à jour le registre des traitements de donnée

Le DPD tient à jour le registre des processus de traitement de données. Ce registre est revu régulièrement en groupe de travail pour identifier si de nouveaux processus de traitement ont été mis en place.

5.2 Effectuer une étude d'impact sur les processus traitant des données personnelles

Pour chaque processus de traitement figurant dans le registre, le DPO réalise une évaluation des risques en utilisant le logiciel PIA mis à disposition par la CNIL.

L'évaluation porte sur les points suivants :

- La finalité du traitement en vérifiant bien qu'il répond soit à une exigence légale, soit à une finalité de l'entreprise qui doit être définie et licite,
- Le type de données traitées, leur sensibilité et leur cycle de vie,
- Les mesures protectrices des droits des personnes sur leurs données personnelles,
- Les risques pouvant entraîner un accès illégitime, une perte ou une destruction de données,
- Les mesures existantes pour réduire ces risques.

Chaque évaluation est réalisée conjointement par le DPD et le service informatique avec le responsable du traitement.

En fonction du risque évalué sur une matrice gravité/vraisemblance, des actions sont décidées (qui, quoi, pour quand) avec le responsable de traitement et le service informatique pour réduire le niveau de risque.

A la fin de l'évaluation, l'avis du DPD et du service informatique est recueilli et noté dans le registre.

L'évaluation et le plan d'action sont transmis au responsable de traitement et au service informatique.

Le plan d'action par traitement est suivi à chaque réunion du groupe de travail. Le critère retenu est le taux d'avancement des actions décidées.

En cas de détection d'un traitement dont la finalité est illicite, le DPD informe la Direction du groupe dans les délais les plus brefs pour qu'une décision soit prise.

5.3 Communiquer en interne et en externe

Une sensibilisation des responsables de traitement est réalisée à l'occasion des évaluations des risques.

Un point trimestriel est réalisé par le DPD au management committee avec notamment un suivi sur l'avancement des actions et sur les processus les plus risqués.

Le personnel de l'entreprise est informé régulièrement de l'avancement de la démarche RGPD au travers du journal interne « Le Petit Messager ».

La politique est également publiée sur le site internet www.metauxspeciaux.fr.

Une communication adaptée est également diffusée à notre actionnaire.

5.4 Former

Un module de formation du personnel sur le RGPD sera développé par le DPD qui en assurera la présentation lors des formations à la sécurité informatique qui seront dispensées par le service informatique. En cas d'empêchement du DPD, cette formation pourra aussi être animée par un autre membre du groupe de travail.

5.5 Sécuriser les contrats avec les sous-traitants

L'entreprise vérifie que les sous-traitants qui traitent des données personnelles s'engagent contractuellement à traiter ces données en conformité avec le RGPD. Elle vérifie si les obligations contractuelles des sous-traitants garantissent un niveau de protection suffisant.

Un niveau de vigilance élevé est porté sur les sous-traitants informatiques qui ont accès à une quantité importante de données (éditeurs de logiciels, prestataires de service, solutions d'hébergement dans le cloud, services en mode SAS, hébergeurs de données), ainsi qu'aux sous-traitants et fournisseurs hébergeant des données en dehors de l'Union Européenne.

En cas de doute sur le niveau de sécurité d'un sous-traitant, un audit pourra être réalisé par le DPD et le service informatique.

5.6 Respecter les droits des personnes physiques.

L'entreprise s'engage à informer les personnes physiques (salariés, clients, fournisseurs, tiers) des données personnelles qu'elle détient sur elles, de la finalité du traitement et de leur droit d'accès à ces données, de rectification et d'effacement.

Quand le traitement n'est pas lié à une obligation légale ou contractuelle, l'entreprise s'engage également à obtenir le consentement des personnes physiques sur l'utilisation qui sera faite de leurs données personnelles. Le recueil de consentement est effectué par le responsable de traitement, après avis du DPD et la preuve de ce recueil est conservée par le responsable de traitement.

5.7 Améliorer les bonnes pratiques informatiques

Suite aux évaluations RGPD et aux audits de sécurité informatique, le service informatique a mis en place :

· Pour les nouveaux arrivants : un cursus d'accueil informatique des nouveaux arrivants avec conseils de sensibilisation à la sécurité informatique et signature de la charte informatique,

· Pour le personnel déjà présent dans l'entreprise : un programme de sensibilisation à la sécurité informatique et tapis de souris rappelant les bonnes pratiques en matière de sécurité informatique.

5.8 Définir des durées d'archivage

Se référer aux procédures d'archivages en vigueur.

5.9 Intervenir en amont dans les projets pour garantir la sécurité des données personnelles

Le DPD peut être sollicité par le responsable de traitement en amont pour tout projet impliquant un nouveau traitement aux données personnelles. Il analyse le traitement envisagé, les données collectées et émet des recommandations auprès du responsable de traitement.

De même, le DPD peut être sollicité par tout salarié sur des sujets de protections de données personnelles (fichiers, dossiers…).

5.10 Sécuriser le transfert de données personnelles hors Union Européenne

Etant partie d'un groupe international, l'entreprise transmet des documents contenant des données personnelles à des entités situées en dehors de l'Union Européenne.

Des clauses contractuelles standards entre l'entreprise et l'entité légale recevant les données sont établies, conformément aux recommandations de la CNIL.

5.11 Informer la CNIL en cas d'accès illégitime aux données

L'entreprise informera la CNIL dans les 48 heures en cas d'accès illégitime de données porté à sa connaissance. L'entreprise vérifiera que cette obligation figure dans les obligations contractuelles de ses sous-traitants.