1. CONTEXTE ET LEADERSHIP

Sur demande du Groupe SFPI, son actionnaire principal, NEU AUTOMATION a déterminé les enjeux internes et externes dans le cadre du contexte RGPD et a identifié les responsabilités liées à la conformité RGPD, en s'appuyant sur la démarche processus existante en tant qu'organisme certifié.

Cette procédure a pour but de formaliser les actions identifiées en matière de conformité, de suivi, d'amélioration, d'analyse de risques et de suivi des incidents et de communiquer à l'ensemble des parties prenantes l'efficacité de ces actions.

2. AUTORITE ET DELEGATION A LA PROTECTION DE LA DONNEE PERSONNELLES

Le Groupe SFPI a nommé un délégué à la protection de la donnée personnelle, dont les compétences ont été évaluées au cours de la première réunion du comité de pilotage. Il s'agit du Directeur de la maitrise des processus de la société DELTA NEU, filiale du Groupe SFPI.

Le dossier CNIL de la personne concernée porte le numéro de dossier DPO-13345 et a donné lieu à une information générale à l'ensemble des responsables de traitement.

3. SUPPORT ET RESSOURCES

Un comité de pilotage Groupe été constitué afin de mettre en place et de suivre les dispositions relatives au RGPD. Ce comité de pilotage est constitué d'un référent pour chacun des quatre pôles d'activités du Groupe, ainsi que d'un membre du comité de Direction de la SFPI. Il se réunit à intervalle régulier dans l'année afin de définir notamment des programmes de sensibilisation et des besoins en communication pour toutes les parties prenantes.

Un répertoire des sociétés éligibles du Groupe est disponible avec des indicateurs permettant d'évaluer l'état d'avancement société par société ou de façon plus globale.

Le comité de pilotage du Groupe SFPI a validé et communiqué à l'ensemble des parties prenantes en français et en Anglais l'ensemble des documents relatifs au règlement, et notamment la politique de sécurité. Le support préconisé pour cette opération de mise à disposition documentaire est le site Internet de chaque société du groupe, éligible au règlement

La réunion de management annuelle DELTA NEU permet de sensibiliser les managers à l'évolution du règlement et des actions menées, à leur charge de diffuser ces informations à leurs collaborateurs.

La Direction de la Maitrise des Processus de DELTA NEU effectue des actions de sensibilisation lors de revues de processus et/ou d'audits internes et/ou de réunions informelles.

Les contrats de travail des jeunes embauchés comportent une clause relative à la protection des données personnelles. Pour les collaborateurs déjà en place, une mention relative à la protection des données personnelles est stipulée au niveau de notre charte d'utilisation du système d'informations et des réseaux sociaux Ces deux documents sont enregistrés comme annexe à notre règlement intérieur.

4. MAITRISE DES TRAITEMENT ET DES DONNES

Les informations inhérentes à la maitrise des traitements et des données sont mises à disposition à travers deux fichiers Excel, NEU AUTOMATION et CSE NEU AUTOMATION, constitués de plusieurs onglets, décrits dans les chapitres suivants.

Un premier onglet décrit les principes du règlement RGPD en termes d'organisation, de conception, d'analyse et d'évolution des traitements, de sécurisation de l'information, de la maitrise de la sous-traitance, des moyens de collecte et de demandes d'exercices de droits des personnes, de détection et traitement des violations de données, de l'efficacité et de l'amélioration du système mis en place.

4.1 REGISTRE DES ACTIVITES DE TRAITEMENT

Le registre des activités de traitement est organisé suivant une démarche processus.

Le Directeur Général est identifié comme le responsable des traitements.

Le représentant du responsable des traitements est identifié le plus souvent comme le pilote du processus concerné.

La notion de responsable conjoint de traitement n'est pas applicable chez NEU AUTOMATION.

Le Directeur de la maitrise des processus de DELTA NEU a la charge de valider les informations relatives au traitement en tant que DPD du Groupe

On retrouve pour chaque processus identifié les informations permettant de décrire l'ensemble des traitements qui s'appuie sur des données personnelles, à savoir :

- Nom, finalité, activité, moyens de pilotage et base juridique du traitement
- Les partie intéressées internes et externes : les différents types de personnes dont nous collectons ou utilisons les données.
- Les données personnelles collectées, sensibles s'il y a lieu.
- Le nom des destinataires des données et dans la mesure du possible la durée de conservation des données
- La notion de transfert de ces données hors UE
- Les mesures de sécurité techniques et organisationnelles des données collectées
- Des informations relatives à la création, mise à jour et validation du contenu
- Les mesures relatives aux sous-traitants concernés par nos traitements sont décrites dans le chapitre 5 de cette procédure

La décision de réaliser ou non une analyse d'impact est notifiée à chaque nouvel enregistrement d'un traitement au niveau du registre des activités avec validation du DPD

4.2 EVALUATION DES RISQUES

Une grille d'évaluation et de maitrise des grilles est disponible au niveau du registre de maitrise des traitements

L'analyse et l'évaluation des risques est effectuée par processus et par domaine.

Les informations concernées sont l'aspect, les risques encourus, la justification de la conformité, les propositions d'amélioration , la référence de l'action, la date de révision.

La note brute est déterminée en fonction de la gravité et de la fréquence, la note nette en fonction du coefficient de pondération relatif au niveau de la maitrise du risque.

Les demandes d'amélioration sont enregistrées en tant qu'action et viennent supprimer le risque ou renforcer le niveau de maitrise opérationnelle si le risque ne peut être supprimé.

4.3 MISE EN CONFORMITE – PLAN D'ACTIONS

Les exigences RGPD sont rappelées.

Une analyse des causes est requise, l'action est en cours, en efficacité, soldée, les critères d'efficacité sont notifiés.

Si besoin, la référence de l'action est reportée sur l'onglet d'analyse et d'évaluation des risques. Le fait de solder l'action peut générer une augmentation du coefficient de maitrise des risques, et ainsi diminuer le risque.

Le registre des traitements évolue en conséquence.

Les moyens de mise en œuvre des actions sont identifiés.

4.4 ANALYSE DE MATURITE

L'analyse se fait par le croisement entre les actions à mettre en place et le niveau de conformité de l'entreprise. Le modèle présenté fait apparaitre 5 niveaux de conformité :

- Fonctionnement de base
- Défini
- Maitrisé
- Optimisé
- Améliorations permanentes

Et les actions de maturation à mettre en place

- Loyauté
- Licéité
- Transparence
- Finalité

- Minimisation
- Limitation
- Exactitude
- Sécurité
- Catégories spéciales, dites données à caractère sensible
- Droits des personnes concernées
- Information des personnes concernées
- Droit à la portabilité
- Droit d'opposition
- Accountabilty : Désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.
- Privacy by design : implique de protéger les données personnelles dès la conception
- Maitrise des sous-traitants
- Registre des traitements
- Les règles d'entreprise contraignantes (BCR - Binding Corporate Rules) pour des transfert de données hors UE
- Existence d'un DPO
- Analyse d'impact
- Notification des violations de données
- Traitement des données à des fin statistiques
- Prohibition de la vente des données personnelles
- Réduction des risques
- Réponses aux réclamations
- Formation – sensibilisation
-

4.5 REGISTRE DE VIOLATION DES DONNEES

Toute violation de données est documentée au niveau d'un registre interne (situation d'urgence) dans lequel sont renseignés les faits concernés par la violation, ainsi que les effets et les actions s'y afférant.

Le responsable de traitement / DPO notifie la violation en question à l'autorité de contrôle compétente, dans les meilleurs délai et, si possible, 72h au plus tard après en avoir pris connaissance.

Les actions sont tracées, ainsi que les réponses de l'autorité compétente.

5. SOUS TRAITANCE ET PARTIE PRENANTE

Les sous-traitants à qui nous passons des commandes sur affaire ou sur stock ne sont pas impactés par ce chapitre de la procédure, les données personnelles se réduisant qu'aux coordonnées de l'émetteur de la dite commande

Les sous-traitants impliqués dans le traitement et l'accès aux données personnelles en nombre sont identifiés, une analyse de risque est réalisée et permet d'identifier deux natures de risques :

- Un risque « normal », ce qui signifie que le sous-traitant :
  - Dispose d'un programme de sécurité fondé sur des normes reconnues et documenté
  - Dispose d'un système de management du risque
  - Fait évoluer continuellement son système d'informations
  - Dispose d'un mécanisme de notification de violation de données
  - Effectue une anonymisation des données personnelles
  - Réalise une sensibilisation sur la protection des données auprès de son personnel
  - S'engage à ne pas sous-traiter tout ou partie de activités relatives aux données personnelles à un autre sous-traitant sans en informer le responsable de traitement
- Un risque élevé, ce qui signifie que le sous-traitant :
  - Effectue un traitement qui porte sur des données sensibles ou des personnes vulnérables
  - Prend des décisions fondées sur un traitement automatisé
  - Héberge des données et/ou implique un transfert de données vers un pays n'offrant pas un régime de protection adéquat, un encadrement et donc requis
  - Doit réaliser d'une analyse d'impact

En cas de risque élevé, il convient de s'assurer que le sous-traitant prend toutes les mesures requises en vertu de l'article 32 du règlement (obtenir les preuves) et de l'évaluer périodiquement afin qu'ils maintiennent la conformité

La gestion du sous-traitant est une activité importante, qui impacte directement le responsable du traitement en cas de non-respect du règlement.

6. COLLECTE ET CONSENTEMENT – DROITS A LA PERSONNE

La collecte des données personnelles est réalisée auprès de chaque visiteur de notre site, si et seulement s'il le souhaite.

L'accord du consentement est notifié au niveau de l'enregistrement des données dans notre logiciel de gestion de la relation client (CRM).

Le retrait du consentement et des informations relatives au demandeur est exécuté à première demande sur présentation d'une pièce d'identité en cours de validité suivant les modalités définies dans notre politique RGPD.

Les dispositions prises pour la suppression des données une fois le délai de conservation dépassé sont décrites dans notre modèle de registre des traitements.

NEU AUTOMATION doit répondre à une personne exerçant ses droits dans les meilleurs délais et identifier que les droits sont respectés

8 MESURES DE PROTECTION

L'analyse et l'évaluation des risques suivant une grille de notation permet de les prioriser, de mettre en place un plan d'amélioration pour chacun des risques significatifs identifiés et d'engager un plan de traitement des mesures de protection, ainsi la traçabilité de tous les accès aux données personnelles est assurée

9 AMELIORATION CONTINUE

Une veille règlementaire est mise en place en fonctions des évolutions du règlement
Le rapport d'audit est enregistré au niveau du registre des traitement, peut donner lieu à des non-conformité et/ou des pistes d'amélioration. Des actions sont mises place pour les solder
L'activité relative au RGPD est considérée comme un processus à part entière est revue au moins une fois l'an dans le cadre de la revue de Direction Qualité – Sécurité- Santé -Environnement