ENOVATION

REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES

POLITIQUE

Version :	1.0
Date de la version :	31/01/2018
Cree par :	Matt Makulski
Approuvé par :	Paul Bachy, Gary Mahon
Niveau confidentialité :	Public

Histoire des changements

Date	Version	Crée par	Description du changement
08/01/2018	0.1	Matt Makulski	Première rédaction
16/01/2018	0.2	Matt Makulski	Mis à jour de classification du document
31/01/2018	1.0	Matt Makulski	Version finale pour publication

Sommaire

1. Objet, champ d'application et utilisateurs

Enovation, ci-après dénommée la «Société», s'efforce de se conformer aux lois et règlements applicables en matière de protection des Données Personnelles dans les pays où la Société est active. Cette Politique énonce les principes de base selon lesquels la Société traite les données personnelles des consommateurs, clients, fournisseurs, partenaires commerciaux, employés et autres personnes, et indique les responsabilités de ses départements commerciaux et de ses employés lors du traitement des données personnelles.
Cette Politique s'applique à la Société et à ses filiales détenues à 100% directement ou indirectement, exerçant des activités dans l'Espace économique européen (EEE) ou traitant les données à caractère personnel des personnes concernées dans l'EEE.
Les utilisateurs de ce document sont tous les employés, permanents ou temporaires, et tous les fournisseurs travaillant pour le compte de la Société.

2. Documents de référence

- EU GDPR 2016/679 (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46 / CE)

2. Définitions

Les définitions suivantes des termes utilisés dans ce document sont tirées de l'article 4 du Règlement général de l'Union européenne sur la protection des données :
Données personnelles : Toute information relative à une personne physique identifiée ou identifiable ("Personne concernée") qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Données personnelles sensibles : Les données personnelles qui, par nature, sont particulièrement sensibles en ce qui concerne les libertés et droits fondamentaux, méritent une protection spécifique car le contexte de leur traitement pourrait créer des risques importants pour les droits et libertés fondamentaux. Ces données personnelles comprennent les données personnelles révélant l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques afin d'identifier de façon unique une personne physique, les données de santé ou les données concernant la vie sexuelle ou orientation sexuelle.

Contrôleur de données : La personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.

Processeur de données : Une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui traite des données personnelles pour le compte d'un responsable du traitement des données.

Traitement : Opération ou ensemble d'opérations effectuées sur des données personnelles ou sur des ensembles de données personnelles, automatisées ou non, telles que la collection, enregistrement, organisation, structuration, stockage, adaptation ou altération, récupération, consultation, utilisation, divulgation par transmission, diffusion ou mise à disposition, alignement ou combinaison, restriction, effacement ou destruction des données.

Anonymisation : Désidentification irréversible des données personnelles de sorte que la personne ne peut être identifiée en utilisant un temps, un coût et une technologie raisonnables, soit par le responsable du traitement, soit par toute autre personne pour identifier cette personne. Les principes du traitement des données personnelles ne s'appliquent pas aux données anonymisées car il ne s'agit plus de données personnelles.

Pseudonymisation : Le traitement de données à caractère personnel de telle sorte que les données à caractère personnel ne peuvent plus être attribuées à une personne concernée sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles.

Les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable. La pseudonymisation réduit, mais n'élimine pas complètement, la capacité de lier des données personnelles à une personne concernée. Comme les données pseudonymisées sont toujours des données personnelles, le traitement
des données pseudonymisées doit être conforme aux principes du traitement des données personnelles.

Traitement transfrontalier des données personnelles : Traitement de données à caractère personnel effectué dans le cadre des activités d'établissements situés dans plusieurs États membres d'un responsable du traitement ou du traitement dans l'Union européenne où le responsable du traitement ou le sous-traitant est établi dans plus d'un État membre; ou le traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un seul établissement d'un responsable du traitement ou d'un processeur dans l'Union, mais qui affecte sensiblement ou est susceptible d'affecter de manière substantielle les personnes concernées dans plus d'un État membre;

Autorité de surveillance : Une autorité publique indépendante établie par un État membre en vertu de l'article 51 du RGPD de l'UE ;

Autorité de surveillance principale: L'autorité de surveillance qui est la principale responsable du traitement d'une activité de traitement de données transfrontalière, par exemple lorsqu'une personne concernée se plaint du traitement de ses données personnelles; il est notamment chargé de recevoir les notifications de violation de données, d'être informé des activités de traitement risquées et aura toute autorité en ce qui concerne ses obligations pour assurer le respect des dispositions du RGPD de l'UE;

Chaque "**autorité de surveillance locale**" conservera sur son propre territoire et surveillera tout traitement local de données affectant les personnes concernées ou effectué par un contrôleur ou un sous-traitant de l'UE ou de l'UE lorsque leur traitement cible des personnes résidant sur son territoire. Leurs tâches et pouvoirs comprennent la conduite d'enquêtes et l'application de mesures administratives et d'amendes, la sensibilisation du public aux risques, règles, sécurité et droits relatifs au traitement des données personnelles, ainsi que l'accès aux locaux du responsable du traitement et du transformateur, y compris tout équipement et moyen de traitement de données.

"Établissement principal en ce qui concerne un responsable du traitement" ayant des établissements dans plusieurs États membres, lieu de son administration centrale dans l'Union, à moins que les décisions relatives aux finalités et aux modalités du traitement des données à caractère personnel ne soient prises dans un autre établissement du l'Union et ce dernier établissement ont le pouvoir de mettre en œuvre de telles décisions, auquel cas l'établissement ayant pris de telles décisions doit être considéré comme l'établissement **principal;**

"Établissement principal en ce qui concerne un processeur" ayant des établissements dans plusieurs États membres, le siège de son administration centrale dans l'Union ou, si le transformateur n'a pas d'administration centrale dans l'Union, l'établissement du transformateur dans l'Union où les activités principales de traitement dans le cadre des activités d'un établissement du transformateur ont lieu dans la mesure où le sous-traitant est soumis à des obligations spécifiques au titre du présent règlement;

Entreprise du groupe : Toute société d'investissement avec sa filiale**.**

4. Principes de base concernant le traitement des données personnelles

Les principes de protection des données définissent les responsabilités fondamentales des organisations qui gèrent des données personnelles. L'article 5 (2) du RGPD stipule que "le responsable du traitement doit être responsable et être en mesure de démontrer le respect des principes".

4.1. Légalité, équité et transparence

Les données personnelles doivent être traitées légalement, équitablement et de manière transparente par rapport à la personne concernée.

4.2. Limitation de l'objet

Les données à caractère personnel doivent être collectées à des fins précises, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

4.3. Minimisation des données

Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux finalités pour lesquelles elles sont traitées. La Société doit appliquer l'anonymisation ou la pseudonymisation aux données personnelles si possible afin de réduire les risques pour les personnes concernées.

4.4. Précision

Les données personnelles doivent être exactes et, si nécessaire, mises à jour ; des mesures raisonnables doivent être prises pour garantir que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, sont effacées ou rectifiées en temps opportun.

4.5. Limitation de la période de stockage

Les données personnelles ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles les données personnelles sont traitées.

4.6. Intégrité et confidentialité

Tenant compte de l'état de la technologie et des autres mesures de sécurité disponibles, du coût de mise en œuvre, de la probabilité et de la gravité des risques, la Société doit utiliser des mesures techniques ou organisationnelles appropriées pour traiter les Données Personnelles, y compris la protection contre la destruction accidentelle ou illicite, la perte, la modification, l'accès non autorisé ou la divulgation

4.7. Responsabilité

Les responsables du traitement des données doivent être responsables et être en mesure de démontrer la conformité aux principes énoncés ci-dessus.

5. Construire la protection des données dans les activités commerciales

Afin de démontrer le respect des principes de protection des données, une organisation doit intégrer la protection des données dans ses activités commerciales.

5.1. Notification aux sujets de données

(Voir la section Recommandations sur le traitement équitable.)

5.2. Choix du sujet de données et consentement

(Voir la section Recommandations sur le traitement équitable.)

5.3. Collection

La Société doit s'efforcer de collecter le moins de données personnelles possible. Si des données personnelles sont collectées auprès d'un tiers, le directeur des ventes / marketing doit s'assurer que les données personnelles sont collectées légalement.

5.4. Utilisation, conservation et élimination

Les objectifs, les méthodes, la limite de stockage et la période de conservation des données personnelles doivent être compatibles avec les informations contenues dans la déclaration générale de protection des données. La Société doit maintenir l'exactitude, l'intégrité, la confidentialité et la pertinence des données personnelles en fonction du but du traitement. Des mécanismes de sécurité adéquats conçus pour protéger les données personnelles doivent être utilisés pour empêcher le vol, l'utilisation abusive ou l'abus de données personnelles, et pour empêcher les violations de données personnelles. Le responsable de la sécurité de l'information est responsable de la conformité aux exigences énumérées dans cette section.

5.5. Divulgation à des tiers

Chaque fois que la Société utilise un fournisseur tiers ou un partenaire commercial pour traiter des données personnelles en son nom, le responsable de la sécurité de l'information doit s'assurer que ce processeur fournira des mesures de sécurité pour protéger les données personnelles appropriées aux risques associés. À cette fin, le questionnaire de conformité GDPR du processeur doit être utilisé.

La Société doit exiger contractuellement que le fournisseur ou le partenaire commercial fournisse le même niveau de protection des données. Le fournisseur ou partenaire ne doit traiter les données personnelles que pour exécuter ses obligations contractuelles envers la Société ou sur les instructions de l'entreprise et pas à d'autres fins. Lorsque la Société traite des données personnelles conjointement avec un tiers indépendant, la Société doit explicitement spécifier ses responsabilités respectives et celles du tiers dans le contrat concerné ou tout autre document juridiquement contraignant, tel que le Contrat de traitement des données du Fournisseur.

5.6. Transfert transfrontalier de données personnelles

Avant de transférer des données personnelles hors de l'Espace économique européen (EEE), des garanties adéquates doivent être utilisées, y compris la signature d'un accord de transfert de données, conformément aux exigences de l'Union européenne et, le cas échéant. L'entité recevant les données personnelles doit respecter les principes de traitement des données personnelles définis dans la procédure de transfert de données transfrontalière.

5.7. Droits d'accès par les sujets de données

En tant que responsable du traitement des données, le responsable de la sécurité de l'information doit fournir aux personnes concernées un mécanisme d'accès raisonnable leur permettant d'accéder à leurs données personnelles et leur permettre de mettre à jour, rectifier, effacer ou transmettre leurs données personnelles si approprié ou requis par la loi. Le mécanisme d'accès sera détaillé dans la procédure de demande d'accès du sujet de données.

5.8. Portabilité des données

Les sujets de données ont le droit de recevoir, sur demande, une copie des données qu'ils nous ont fournies dans un format structuré et de transmettre ces données à un autre contrôleur, gratuitement. Le responsable de la sécurité de l'information est responsable de s'assurer que ces demandes sont traitées dans un délai d'un mois, ne sont pas excessives et n'affectent pas les droits des données personnelles d'autres personnes.

5.9. Droit d'être oublié

Sur demande, les sujets de données ont le droit d'obtenir de la Société l'effacement de ses données personnelles. Lorsque la Société agit en tant que Contrôleur, le Responsable de la sécurité de l'information doit prendre les mesures nécessaires (y compris des mesures techniques) pour informer les tiers qui utilisent ou traitent ces données pour se conformer à la demande.

6. Directives de traitement équitable

Les données personnelles ne doivent être traitées que lorsqu'elles sont explicitement autorisées par le Manager de la sécurité des informations.

La Société doit décider d'effectuer ou non l'évaluation de l'impact de la protection des données pour chaque activité de traitement des données conformément aux directives relatives à l'analyse d'impact de la protection des données.

6.1. Avis aux sujets de données

Au moment de la collecte ou avant la collecte de données personnelles pour tout type d'activités de traitement, y compris mais sans s'y limiter, la vente de produits, services ou activités marketing, le directeur des ventes / marketing est responsable d'informer correctement les personnes concernées: types de données personnelles collectées, les finalités du traitement, les modalités de traitement, les droits des personnes concernées vis-à-vis de leurs données personnelles, la période de conservation, les éventuels transferts internationaux de données, si des données sont partagées avec des tiers. Cette information est fournie par l'avis général de protection des données.

Lorsque des données personnelles sont partagées avec un tiers, le responsable de la sécurité de l'information doit s'assurer que les personnes concernées en ont été averties par un avis général de protection des données.

Lorsque des données personnelles sont transférées vers un pays tiers conformément à la politique de transfert de données transfrontalière, la déclaration générale de protection des données doit refléter cette situation et indiquer clairement où et à quelle entité les données personnelles sont transférées.

Lorsque des données personnelles sensibles sont collectées, le responsable de la sécurité de l'information doit s'assurer que la déclaration générale de protection des données indique explicitement le but pour lequel ces données personnelles sensibles sont collectées.

6.2. Obtention des consentements

Chaque fois que le traitement des données personnelles est basé sur le consentement de la personne concernée, ou sur d'autres motifs légitimes, le responsable de la sécurité de l'information est responsable de conserver un enregistrement de ce consentement. Le responsable de la sécurité de l'information est chargé de fournir aux personnes concernées des options pour fournir le consentement et doit informer et s'assurer que leur consentement (chaque fois que le consentement est utilisé comme motif légal de traitement) peut être retiré à tout moment.

Les données personnelles ne doivent être traitées que dans le but pour lequel elles ont été collectées à l'origine. Dans le cas où la Société souhaite traiter des données personnelles collectées à d'autres fins, la Société doit demander le consentement de ses personnes concernées par écrit de façon claire et concise. Toute demande de ce type devrait inclure l'objectif initial pour lequel les données ont été collectées, ainsi que le ou les nouveaux objectifs. La demande doit également inclure la(es) raison(s) du changement de finalité. Le responsable de la sécurité de l'information est responsable du respect des règles de ce paragraphe.

Actuellement et à l'avenir, le responsable de la sécurité de l'information doit s'assurer que les méthodes de collecte sont conformes à la législation pertinente, aux bonnes pratiques et aux normes de l'industrie.

Le responsable de la sécurité de l'information est responsable de la création et du maintien d'un registre des avis généraux de protection des données.

7. Organisation et responsabilités

La responsabilité d'assurer un traitement adéquat des données personnelles incombe à toute personne travaillant pour ou avec la Société et ayant accès aux données personnelles traitées par la Société. Les principaux domaines de responsabilité pour le traitement des données personnelles résident dans les rôles organisationnels suivants :

Le conseil d'administration prend des décisions et approuve les stratégies générales de la Société en matière de protection des données personnelles.

Le **responsable de la sécurité de l'information** est responsable de la gestion du programme de protection des données personnelles et est responsable du développement et de la promotion de politiques de protection des données personnelles de bout en bout. surveille et analyse les lois sur les données personnelles et les modifications de la réglementation, élabore des exigences de conformité et aide les services commerciaux à atteindre leurs objectifs en matière de données personnelles. Il est également chargé de transmettre les responsabilités de protection des données personnelles aux fournisseurs et d'améliorer le niveau de sensibilisation des fournisseurs à la protection des données personnelles, ainsi que de transmettre les exigences relatives aux données personnelles à tout fournisseur tiers. Le service des achats doit s'assurer que la société se réserve le droit de vérifier les fournisseurs.

Le **responsable informatique** est responsable de

- S'assurer que tous les systèmes, services et équipements utilisés pour stocker les données répondent à des normes de sécurité acceptables.
- Effectuer des vérifications et des analyses régulières pour s'assurer que le matériel et les logiciels de sécurité fonctionnent correctement.

Le **responsable marketing** est responsable de :

- Approuver toute déclaration de protection des données jointe à des communications telles que des courriels et des lettres.
- Répondre aux questions de protection des données des journalistes ou des médias comme les journaux.
- Si nécessaire, travailler avec le responsable de la sécurité de l'information pour s'assurer que les initiatives de marketing respectent les principes de protection des données.

Le **directeur des opérations** est responsable de:

- Améliorer la sensibilisation de tous les employés à la protection des données personnelles des utilisateurs.

- Organisation d'une expertise en protection des données personnelles et d'une formation de sensibilisation pour les employés travaillant avec des données personnelles.
- Protection des données personnelles des employés de bout en bout. Il doit veiller à ce que les données personnelles des employés soient traitées en fonction des objectifs commerciaux légitimes et de la nécessité de l'employeur.

8. Directives pour l'établissement de l'autorité de surveillance principale

8.1. Nécessité d'établir l'autorité de surveillance principale

L'identification d'une autorité de surveillance principale n'est pertinente que si la Société effectue le traitement transfrontalier des données personnelles.

Le traitement transfrontalier des données personnelles est effectué si:

a) le traitement des données à caractère personnel est effectué par des filiales de la Société basées dans d'autres États membres;

ou

b) le traitement de données à caractère personnel qui a lieu dans un établissement unique de la Société dans l'Union européenne, mais qui affecte sensiblement ou est susceptible d'affecter substantiellement les personnes concernées dans plus d'un État membre.

Si la société n'a que des établissements dans un État membre et que ses activités de traitement n'affectent que les personnes concernées dans cet État membre, il n'est pas nécessaire de créer une autorité de surveillance principale. La seule autorité compétente sera l'autorité de surveillance dans le pays où la société est légalement établie.

8.2. L'Établissement principal et l'autorité de surveillance principale

8.2.1. Établissement principal pour le contrôleur de données

Le conseil d'administration doit identifier l'établissement principal afin que l'autorité de surveillance principale puisse être déterminée.

Si la Société est basée dans un État membre de l'UE et prend des décisions relatives aux activités de traitement transfrontalier à la place de son administration centrale, il y aura une seule autorité de surveillance principale pour les activités de traitement des données effectuées par la Société.
Si la Société a plusieurs établissements qui agissent indépendamment et prennent des décisions concernant les finalités et les moyens du traitement des données personnelles, le conseil d'administration doit reconnaître qu'il existe plusieurs autorités de surveillance

8.2.2. Établissement principal pour le processeur de données

Lorsque la Société agit en tant que processeur de données, l'établissement principal sera le siège de l'administration centrale. Dans le cas où la place de l'administration centrale n'est pas située dans l'UE, l'établissement principal sera l'établissement dans l'UE où les principales activités de traitement ont lieu.

8.2.3. Établissement principal pour les entreprises non-UE pour les contrôleurs de données et les processeurs

Si la société n'a pas d'établissement principal dans l'UE et qu'elle a des filiales dans l'UE, l'autorité de surveillance compétente est l'autorité de surveillance locale.

Si la société n'a pas d'établissement principal dans l'UE ni de filiales dans l'UE, elle doit désigner un représentant dans l'UE, et l'autorité de surveillance compétente sera l'autorité de surveillance locale où le représentant est situé.

9. Réponse aux incidents de violation de données personnelles

Lorsque la société apprend qu'une violation de données personnelles est suspectée ou réelle, le responsable de la sécurité de l'information doit mener une enquête interne et prendre les mesures correctives appropriées en temps opportun, conformément à la politique de violation des données. En cas de risque pour les droits et libertés des personnes concernées, la Société doit en informer les autorités compétentes en matière de protection des données sans retard injustifié et, si possible, dans les 72 heures.

10. Vérification et responsabilisation

La Société fera appel à des consultants externes qualifiés pour vérifier dans quelle mesure les services commerciaux mettent en œuvre cette politique.

Tout employé qui enfreint cette politique sera passible de mesures disciplinaires et l'employé peut également être passible de poursuites civiles ou pénales si sa conduite enfreint les lois ou les règlements.

11. Conflits de lois

Cette politique est destinée à être conforme aux lois et règlements du lieu d'établissement et des pays dans lesquels Enovation opère. En cas de conflit entre la présente Politique et les lois et règlements applicables, ces derniers prévaudront.

12. Validité et gestion de documents

Ce document est valable à partir du 31/01/2018.

Le propriétaire de ce document est le gestionnaire de la sécurité de l'information, qui doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an.