Politique de protection et confidentialité des données personnelles

TABLE DES MATIERES

Orientation d'implémentation
Finalité de ce document Ce document détermine les responsabilités de l'organisation et la politique de confidentialité et protection des données personnelles.
Domaines et articles du RGPD traités: Chapitre II - Principes Chapitre IV – Responsable du traitement et Sous-traitant, articles 24 à 31.
Révision Ce document sera révisé annuellement, sans préjudice des modifications dues à des changements de la législation, de la réglementation, ou à des transformations majeures dans l'organisation.

1 INTRODUCTION

Dans le cadre de son activité, SteelPlus utilise une variété des données concernant des personnes identifiables, y compris des données portant sur:

- Clients
- Fournisseurs
- Partenaires commerciaux
- Entités sous-traitantes
- Collaborateurs

En effectuant la collecte et l'usage de ces données, SteelPlus est soumise à plusieurs obligations, découlant des lois et règlements qui concernent la manière selon laquelle ces activités peuvent être effectuées et les contrôles nécessaires pour garantir leur protection. La finalité de cette politique est de déterminer la législation pertinente et décrire les procédures pour assurer la conformité de SteelPlus à la législation applicable.

Ces procédures sont d'application générale, soit à tous les systèmes et processus qui, dans son ensemble, constituent le système d'information de SteelPlus, soit à tous les Collaborateurs, membres des organes sociaux, fournisseurs et d'éventuels tiers ayant accès aux systèmes de SteelPlus.

2 POLITIQUE DE CONFIDENTIALITE ET PROTECTION DES DONNEES PERSONNELLES

2.1 REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES

Le Règlement général sur la protection des données (désormais, RGPD) a été approuvé par la Commission européenne (CE) le 27 avril 2016 et est entré pleinement en vigueur le 25 mai 2018. Ce Règlement remplace la législation antérieure de la CE, concernant la protection des données, et une de ses principales caractéristiques c'est qu'il s'agit d'un Règlement et pas une Directive, ce qui signifie qu'il *devient loi* automatiquement dans chacun des pays formant l'Union européenne, sans qu'il soit nécessaire que chacun de ces pays établissent ses propres lois internes.

Le RGPD a été créé pour la protection des données personnelles des citoyens de l'Union européenne. Ainsi, il s'agit d'une des principales législations qui affectent la manière selon laquelle les entités effectuent leurs activités de traitement des informations concernant les données personnelles. Le RGPD détermine des amendes importantes en cas de violation, raison pour laquelle il est une politique de SteelPlus la garantie de l'adhésion totale et la conformité au RGPD et autres législations et réglementations pertinentes.

2.2 FORMAT DU REGLEMENT

Le RGPD dispose de quatre-vingt-huit pages et est divisé en deux parties principales:

- 1ère. Partie composée par Considérants - 173 paragraphes numérotés déterminant les principes et les finalités du règlement;
- 2ème. Partie composée par Articles - 99 articles définissant les détails du Règlement - la partie qui doit être accomplie.

2.3 DEFINITIONS

Le RGPD détermine, dans son ensemble, 26 définitions:

a) «Données personnelles», information concernant une personne physique identifiée ou identifiable («titulaire de données»); il est considéré comme identifiable une personne physique 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, des identifiants en ligne, ou à un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique;

b) «Traitement», une opération ou un ensemble d'opérations effectuées à des données ou des ensembles de données personnelles, par des moyens automatisés ou non automatisés, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'aménagement ou la modification, la récupération, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

c) «Limitation du traitement», l'apposition d'une marque sur des données personnelles conservées, en vue de limiter leur traitement futur;

d) «Profilage», toute forme de traitement automatisé de données personnelles consistant à utiliser ces données personnelles pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou anticiper des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements;

e) «Pseudonymisation», le traitement des données personnelles de telle façon que celles-ci ne puissent plus être attribuées à un titulaire de données précis sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles à fin de garantir que les données personnelles ne puissent pas être attribuées à une personne physique identifiée ou identifiable;

f) «Fichier», tout ensemble structuré de données personnelles accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

g) «Responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

h) «Sous-traitant», une personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte du responsable du traitement;

i) «Destinataire», une personne physique ou morale, l'autorité publique, le service ou un autre organisme qui reçoit communication de données personnelles, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données personnelles dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question doit répondre aux règles de protection des données en fonction des finalités du traitement;

j) «Tiers», la personne physique ou morale, l'autorité publique, le service ou un organisme autre que le titulaire de données, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données personnelles

k) «Consentement» du titulaire de données, une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle le titulaire de données accepte, par une déclaration ou par un acte positif clair, que des données personnelles le concernant fassent l'objet d'un traitement;

l) «Violation de données personnelles», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à de données personnelles transmises, conservées ou traitées d'une autre manière;

m) «Données génétiques», les données personnelles relatives aux caractéristiques génétiques, héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

n) «Données biométriques», les données personnelles résultantes d'un traitement technique spécifique, relatif aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

o) «Données concernant la santé», les données personnelles relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur son état de santé;

p) «Établissement principal», a) en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données personnelles soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement ait le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal; b) en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans

l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement;

q) «Représentant», une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui représente le responsable du traitement ou le sous-traitant en ce qui concerne leurs obligations respectives en vertu du présent règlement;

r) «Entreprise», une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

s) «Groupe d'entreprises», un groupe composé d'une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle;

t) «Règles d'entreprise contraignantes», les règles internes de protection des données personnelles qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données personnelles à un responsable du traitement ou à un sous-traitant dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe;

u) «Autorité de contrôle», une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51;

v) «Autorité de contrôle concernée», une autorité de contrôle qui est concernée par le traitement de données personnelles parce que: a) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève; b) les titulaires de données résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectés par le traitement des données, ou sont susceptibles de l'être; ou c) une réclamation a été introduite auprès de cette autorité de contrôle;

w) «Traitement transfrontalier», a) le traitement de données personnelles qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États

membres; ou b) le traitement de données personnelles qui a lieu dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des titulaires de données dans plusieurs États membres;

x) «Objection pertinente et motivée», une objection à un projet de décision quant à savoir s'il y a ou non violation du présent règlement ou si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant respecte le présent règlement, qui démontre clairement l'importance des risques que présente le projet de décision pour les libertés et droits fondamentaux des titulaires de données et, le cas échéant, pour le libre flux des données personnelles au sein de l'Union;

y) «Service de la société de l'information», un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil (1);

z) «Organisation internationale», une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

2.4 PRINCIPES RELATIFS AU TRAITEMENT DES DONNEES PERSONNELLES

Le RGPD détermine une série des principes fondamentaux concernant le traitement des données personnelles, raison pour laquelle ce traitement doit être:

a) Licite, loyal et transparent au regard du titulaire des donnés («licéité, loyauté et transparence»);

b) Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales («limitation des finalités»);

c) Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles les données sont traitées («minimisation des données»);

d) Exact et, si nécessaire, tenu à jour; toutes les mesures raisonnables doivent être prises pour que les données personnelles qui sont inexactes, eu égard aux finalités

pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder («exactitude»);

e) conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles les données sont traitées; les données personnelles peuvent être conservées pour des durées plus longues dans la mesure où les données personnelles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées («limitation de la conservation»);

f) traitées de manière à assurer une sécurité appropriée des données personnelles, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées («intégrité et confidentialité»).

SteelPlus assure la conformité de son activité aux tous ces principes, en concernant aussi bien le traitement des données effectué actuellement que l'introduction de nouvelles méthodes potentiels.

2.5 DROITS DES TITULAIRES DE DONNEES

Dans le cadre du RGPD, les titulaires de données disposent des droits suivants:

1. Droit d'être informé
2. Droit d'accès
3. Droit de rectification
4. Droit à l'effacement
5. Droit à la limitation du traitement
6. Droit à la portabilité des données
7. Droit d'opposition
8. Droit concernant la prise de décision et le profilage.

Chacun de ses droits dispose des procédures spécifiques pour leur mise en œuvre, lesquelles obligent SteelPlus à prendre des mesures dans les délais présentés dans le RGPD.

Exercice des droits du titulaire de données	Délai
Droit d'être informé	Lorsque les données sont collectées (si fournies par le titulaire de droits) ou dans le délai d'un mois (si les données n'ont pas été fournies par le titulaire de droits)
Droit d'accès	Un mois
Droit de rectification	Un mois
Droit à l'effacement	Sans retard indu
Droit à la limitation du traitement	Sans retard indu
Droit à la portabilité des données	Un mois
Droit d'opposition	Lorsque l'opposition a été reçue
Droit concernant la prise de décisions et le profilage.	Non spécifié

2.6 LICEITE DU TRAITEMENT DES DONNEES PERSONNELLES

Le RGPD détermine six manières alternatives pour régler la licéité du traitement de données, lesquelles sont brièvement présentées ci-dessous. Il est une politique de SteelPlus d'identifier la base appropriée pour le traitement et la documenter.

2.6.1 Consentement

Sans préjudice de toute autre forme de collecte légale des données autorisée par le RGPD, SteelPlus obtiendra toujours le consentement explicite d'un titulaire de données pour collecter et traiter ses données. Le moment où le consentement est obtenu, des informations transparentes seront fournies aux titulaires de données concernant notre utilisation des données; ils seront aussi informés de leurs droits. Cette information sera présentée de manière claire, transparente et gratuite. Si les données personnelles n'ont pas été obtenues auprès du titulaire de données, ces informations seront fournies au titulaire de données dans un délai raisonnable après la collecte des données.

2.6.2 Exécution d'un contrat (ou des mesures pré contractuelles)

Lorsque les données personnelles collectées et traitées sont nécessaires à fin d'accomplir un contrat avec le titulaire de données, il ne faut pas le consentement explicite.

Celui-ci sera normalement le cas de SteelPlus; les Contrats conclus, résultants de l'exercice de son activité, ne peuvent pas être complétés sans les données personnelles concernées.

2.6.3 Accomplissement d'une obligation légale

Si les données personnelles doivent être collectées et traitées pour accomplir une obligation légale, il ne faut pas le consentement explicite. Celui-ci sera normalement le cas de SteelPlus, étant soumise à une obligation réglementaire d'évaluation de la solvabilité et la capacité économique et financière de ses clients, résultants de l'exercice de son activité. Celui-ci peut être aussi le cas de SteelPlus en concernant les données relatives à des Collaborateurs, par rapport à la législation du travail qu'il faut respecter, ainsi que d'autres situations résultantes de sa relation avec des entités publiques (par exemple: Sécurité sociale, Autorité fiscale).

2.6.4 Sauvegarde des intérêts vitaux des titulaires de données

Lorsque les données personnelles sont nécessaires pour protéger les intérêts vitaux du titulaire de données.

2.6.5 Mission d'intérêt public

Quand il s'agit de la mise en œuvre d'une mission d'intérêt public ou effectuée par une autorité publique.

2.6.6 Intérêts légitimes

Si le traitement des données personnelles spécifiques est de l'intérêt légitime du responsable du traitement, sans affecter les droits et libertés du titulaire de données de manière significative.

2.7 PRINCIPE DU RESPECT DE LA VIE PRIVEE DES LA CONCEPTION "PRIVACY BY DESIGN"

SteelPlus adopte le principe du respect de la vie privée dès la conception et assure que la définition et la planification de tous les systèmes nouveaux ou sensiblement modifiés

qui collectent ou traitent des données personnelles seront soumises à l'attention nécessaire concernant des questions de respect de la vie privée, y compris les respectives analyses d'impact de la protection des données. L'analyse d'impact de la protection des données affecte les points suivants:

- Prise en compte de la manière selon laquelle les données personnelles seront traitées et avec quelles finalités;
- Analyse de la nécessité du traitement proposé, ainsi que sa compatibilité avec la finalité;
- Analyse des risques pour les personnes dans le traitement des données personnelles;
- Les contrôles nécessaires pour traiter les risques identifiés et démontrer la conformité à la législation;
- L'usage de techniques comme la minimisation des données et la pseudonymisation, le cas échéant.

2.8 CONTRATS IMPLIQUANT LE TRAITEMENT DES DONNEES PERSONNELLES

SteelPlus assure que tous les contrats impliquant le traitement des données personnelles sont documentés et disposent des clauses spécifiques sur la protection des données.

2.9 TRANSFERTS INTERNATIONAUX DE DONNEES PERSONNELLES

SteelPlus ne transfère pas des données au dehors de l'Union Européenne. Dans ce cas, les transferts seront soigneusement examinés avant qu'ils s'effectuent, de sorte à assurer qu'ils sont en conformité aux exigences du RGPD et des réglementations connexes.

2.10 RESPONSABLE DE LA PROTECTION DES DONNEES

Le RGPD exige la définition d'un Responsable de la Protection des Données (DPO) pour les autorités publiques, en concernant des entités effectuant des traitements des données à grande échelle ou des entités effectuant des traitements des données particulièrement sensibles à grande échelle.

2.11 NOTIFICATION DES VIOLATIONS

Selon le RGPD, lorsqu'il y a la connaissance qu'il a eu une violation pouvant entraîner des risques pour les droits et libertés des personnes, l'autorité de surveillance compétente en sera informée dans un délai de 72 heures. Il est une politique de SteelPlus d'être juste et équitable en la considération de quelles actions doivent être implémentées pour informer les parties concernées par rapport à des violations des données personnelles.

2.12 CONFORMITE AU RGPD

Pour assurer que SteelPlus soit toujours en conformité au principe de responsabilité permanente du RGPD, les actions suivantes seront toujours implémentées:

- La base juridique au traitement des données personnelles est claire et univoque;
- Il est désigné un responsable de la protection des données;
- Tous les Collaborateurs qui aient accès à des données personnelles respectent les bonnes pratiques de la protection des données;
- Formation en protection des données;
- Si nécessaire, il y aura des règles sur le consentement;
- Il y a des formulaires pour que les titulaires de données puissent exercer leurs droits et ces demandes sont traitées de manière efficace;
- Il y a des politiques de confidentialité;
- Des révisions régulières sont effectuées aux procédures concernant les données personnelles;
- Le "*principe du respect de la vie privée dès la conception" (by design")* est adopté par tous les systèmes et processus nouveaux ou modifiés.