DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

CHARTE DE SECURITE DE LA DONNEE ET SENSIBILISATION RGPD

I. PREAMBULE

A. *Qu'est-ce que le RGPD ?*

Le sigle RGPD signifie « Règlement Général sur la protection des données ». Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française « Informatique et Liberté » de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données le concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs (CNIL).

B. *Qu'est-ce qu'une donnée personnelle ?*

Toujours selon la CNIL, une donnée personnelle est « *toute information se rapportant à une personne physique identifiée ou identifiable* ». Une personne peut être identifiée soit directement (Nom, prénom…) ou indirectement (Numéro de téléphone, numéro d'identifiant…).

C. *Qu'est-ce qu'un traitement de donnée personnelle ?*

La CNIL définie le traitement de donnée personnelle comme « *une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé* ».

Par exemple, le traitement d'une donnée personnelle peut être la tenue d'un fichier clients, la collecte de coordonnées de prospects via un questionnaire ou encore la mise à jour d'un fichier de fournisseurs…

S'il n'est pas interdit de traiter de la donnée personnelle, celui-ci doit avoir un objectif qu'on appelle finalité. Aussi, il est interdit de collecter ou traiter des données personnelles simplement au cas où cela puisse avoir une utilité un jour. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle.

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

D. *Qui est le contact concernant les demande RGPD ?*

C'est le DPO (Data Protection Officer ou délégué à la protection des données). Il est en charge de répondre à toutes les questions concernant le RGPD, soit directement, soit en faisant le relais avec le bon interlocuteur.

II. NOTRE CHARTE DE BONNES PRATIQUES

A. *Rappel*

STECO met en œuvre un système d'information et de communication nécessaire à son activité. Tout utilisateur du système d'information devra, dans l'exercice de ses fonctions ou de ses missions, utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'entreprise.

La présente Charte prescrit en partie les règles et usages d'utilisation des ressources informatiques de STECO ainsi que des préconisations en matière de sécurité de l'information. Elles sont applicables aux intervenants internes et extérieurs personnes physiques ou morale, et ce quel que soit leur statut.

L'intervenant, personne physique ou morale, devra avoir pris connaissance de la présente Charte et s'engager à en respecter le contenu en signant le présent document avant de commencer l'exécution de sa mission au profit de STECO.

Cette dernière dispose d'un aspect réglementaire. Elle ne se substitue en aucun cas aux lois en vigueur.

B. *L'objet de la charte*

La Charte a pour objet de définir les règles et précautions d'utilisation des ressources informatiques, ainsi que des informations et données qu'elles contiennent ou véhiculent, et plus largement des règles relatives au traitement de la donnée personnelle.

Définitions : Les termes ci-après, qu'ils soient au pluriel ou au singulier, devront être entendus selon les définitions suivantes.

Utilisateur **:** toute personne, quel que soit son statut (Associés et salariés de l'entreprise, salarié d'une entreprise extérieure, intérimaire, stagiaire…) ayant accès aux ressources informatiques de STECO, ainsi qu'aux informations qu'elles contiennent.

Support informatiques **:** l'ensemble des éléments matériels et logiciels qui permettent notamment le transfert, la mémorisation, la saisie, l'affichage, la communication, l'impression ou le traitement informatisé de l'information (tels que les réseaux, les serveurs, les micro-ordinateurs fixes et portables (y compris les assistants portables numériques – PDA – Smartphones etc.), les scanners, les imprimantes, les applications métiers, les systèmes d'exploitation, les logiciels de bureautique et de communication, etc.), appartenant à STECO ou mis à disposition de STECO à titre gratuit ou onéreux par des tiers, qu'ils soient situés dans les locaux de STECO ou en dehors.

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

Informations : l'ensemble des informations et données accessibles par les ressources informatiques ou papiers, qu'elles soient réputées confidentielles ou non, quelle que soit sa forme et son historique, pour l'application de la présente Charte.

Ressources : les Ressources sont composées du Support ainsi que des Informations.

Données nominatives : il s'agit, au sens de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi dite Informatique et Libertés), des informations qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques (agent de l'entreprise, client, stagiaires etc.) auxquelles elles s'appliquent.

C. *Principes généraux*

a. Principes généraux applicables à l'utilisation des Ressources

La sécurité informatique et des données dans l'entreprise est un objectif qui doit être partagé par tous et qui nécessite la responsabilisation de chaque Utilisateur.

Ainsi, chaque Utilisateur est responsable de l'utilisation qu'il fait de tout type de Ressources auquel il pourrait avoir accès, qu'elles soient locales ou distantes. L'utilisateur s'engage à veiller et à contribuer à la sécurité générale de ces ressources, à la confidentialité et à la qualité des Informations qu'elles contiennent. Il se doit de respecter la législation applicable (notamment la loi dite Informatique et Libertés, les droits relatifs à la propriété intellectuelle, le droit de propriété, les interdictions relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, etc…).

L'utilisateur se doit également de transmettre toute irrégularité liée aux droits, usages, mouvements concernant des Informations.

Les Ressources mises à disposition sont et demeurent la propriété STECO.

Les informations créées ou mises à disposition via des Ressources informatiques sont et demeurent la propriété de STECO.

Toutes créations issues des Informations propriété de STECO sont et demeurent la propriété de STECO.

b. Principes généraux applicables à l'utilisation des Informations

L'utilisateur s'engage à respecter la confidentialité de l'ensemble des Informations dont il pourrait avoir connaissance grâce aux Ressources informatiques. De plus, L'utilisateur s'engage à tout mettre en œuvre pour préserver la confidentialité du processus d'accès à ces Informations.

L'utilisateur s'interdit par conséquent de divulguer ou de céder directement ou indirectement tout ou partie des Informations à tout tiers, que ce soit à titre gracieux ou onéreux.

L'utilisateur s'interdit de faire usage des Informations d'une manière qui pourrait porter préjudice à STECO. Il s'interdit notamment d'en user dans le but de concurrencer cette dernière.

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

L'utilisateur s'interdit d'effectuer le partage, l'exportation, une copie ou tout autre mode de reproduction des Informations dont il aurait connaissance à l'occasion de l'exécution de sa mission, à l'exclusion de celles qui sont indispensables à l'accomplissement de sa mission.

L'utilisateur s'interdit l'importation de Ressources informatiques non-liées à l'utilisation et à l'usage de cette dernière sans l'accord préalable et écrit du Responsable de la Ressource informatique.

L'utilisateur avisera STECO dans les meilleurs délais de tout usage ou divulgation non autorisé, qu'il soit avéré ou suspecté et que cela soit fait par L'utilisateur directement mais également par un tiers.

Dès lors que L'utilisateur a achevé sa mission, ce dernier s'engage à ne pas conserver les Informations dont il aurait eu connaissance, de manière directe ou indirecte, à l'occasion de l'exécution de sa mission. De plus, L'utilisateur doit être en mesure, en cas de contrôle par la personne (physique ou morale) compétente, de justifier l'utilisation et l'usage qui a été fait des Ressources informatiques.

D. Conditions d'utilisation des Ressources informatiques et sécurité

a. Rôle de L'utilisateur

L'utilisateur limite l'utilisation de la ressource aux seules fins de son activité. Il a le devoir de confidentialité et de signalement comme défini dans le présent document.

b. Rôle de l'entreprise

L'entreprise met en œuvre les moyens humains et techniques appropriés pour permettre à l'utilisateur d'assurer la sécurité matérielle et logicielle du système d'information et de communication.

À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

La mise en place et la révision du périmètre d'accès aux Ressources informatiques est sous la responsabilité de la personne compétente. Ainsi, le Responsable de la ressource est en charge de sa mise en œuvre.

La personne compétente a l'obligation de modifier ce périmètre, si cela s'avère nécessaire au regard d'un changement d'utilisation ou d'usage de l'Information et/ou de la Ressource informatique dans les délais appropriés et sans nécessairement prévenir les utilisateurs.

c. Règles d'utilisation des identifiants d'accès et mots de passe

Les habilitations pour l'accès aux Ressources informatiques de STECO sont attribuées et modifiées par ce dernier en considération de la présente Charte et en tenant compte des nécessités de continuité de service.

Les mots de passe sont personnels et confidentiels. Ils ne doivent être divulgués à aucun tiers (ni en interne, ni en externe).

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

L'utilisateur veillera à le changer régulièrement même quand le système ne l'y contraint pas (à minima une fois par an) et, à tout moment, sur simple demande du Responsable de la ressource informatique.

L'accès attribué à un intervenant externe ou bien à contrat à durée déterminée (ex : intérimaire, prestataire etc.) est personnel, temporaire et limité à la mission qui lui est confiée.

Chaque utilisateur est responsable de l'utilisation, de l'usage et des usages de ses identifiants et mots de passe.

d. Préservation de l'intégrité du système informatique

L'utilisateur est dans l'obligation de ne pas mettre en œuvre des utilisations et/ou usages qui seraient susceptibles d'altérer, directement ou indirectement, l'intégrité et/ou la cohérence des Ressources Informatiques.

Si l'utilisateur constate un dysfonctionnement, une anomalie ou toute autre atteinte à l'intégrité et/ou la cohérence de la Ressource informatique, il doit en avertir le Responsable de la Ressource informatique.

e. Respect de la confidentialité et de l'intégrité et/ou la cohérence des Informations

En complément de ce qui a été énoncé précédemment, si des Ressources informatiques sont accessibles pour un utilisateur non-habilité, ce dernier se doit de ne pas utiliser et de ne pas user de cette Ressource informatique.

Toutes les Ressources informatiques qui ne sont pas localisées dans des emplacements maintenus par le Responsable de la ressource ne sont pas sauvegardées (Notamment, tout ce qui se trouve sur les lecteurs locaux des postes utilisateurs). Toute constatation par un utilisateur de l'altération de l'intégrité et/ou de la cohérence d'une Ressource informatique doit être signalée au plus tôt au responsable de la Ressource informatique.

E. Données personnelles

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par la Gérance et applicables quel que soit le support de communication utilisé.

L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à l'entreprise, dans des lieux autres que ceux habituels de travail (hôtel, espaces de co-working,..).

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Tout utilisateur pourra avoir accès aux données le concernant et ces données ne seront conservées que sur une période maximale de 10 ans après la fin du dernier élément contractuel le reliant à STECO, exception faite des cas ou là loi/réglementation, impose une conservation plus importante.

Dans le cadre du Règlement européen sur la protection des données entré en vigueur le 25 mai 2018, le cadre légal concernant la protection des données personnelles s'est considérablement étoffé. Cette mise en conformité à ce nouveau cadre permet d'ajouter des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Également cela permet de protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel. En effet, l'entreprise, par le biais de différents moyens et documents met tout en œuvre pour protéger les données collectées et permettre aux personnes concernées de pouvoir y accéder ou plus généralement de pouvoir exercer leurs droits concernant ces données.

Pour plus d'informations concernant le traitement des données personnelles vous pouvez contacter notre Référent RGPD (DPO) :

- Par courrier électronique : rgpd@steco.fr
- Par courrier postal à l'adresse suivante : RGPD – STECO, 5 rue François Hennebique 17140 LAGORD

Si vous estimez, après nous avoir contactés, que vos droits Informatiques et Libertés ne sont pas respectés, vous pouvez adresser une réclamation en ligne à la CNIL ou par courrier postal.

F. Conditions d'utilisation des réseaux internet

Les utilisateurs s'assurent de la sécurité des réseaux internet auxquels ils se raccordent.

Seront privilégiés les réseaux connus et sécurisés et l'utilisation de réseaux communs strictement limités à la gestion d'un besoin urgent.

G. Conditions d'utilisation de la messagerie électronique

a. Conseils généraux d'utilisation de la messagerie électronique

L'utilisateur s'astreindra, dans les échanges électroniques effectués à l'aide de la messagerie, à la réserve, la discrétion et au respect de la plus grande correction et courtoisie à l'égard de ses interlocuteurs.

Il veillera également à préserver le secret professionnel en toutes circonstances et, a fortiori, lorsque le dossier concerné est couvert par une obligation de confidentialité générale ou spécifique.

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

Par ailleurs, L'utilisateur s'imposera le respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, et celles relatives aux harcèlements sexuel et moral, et doit s'abstenir de porter atteinte à l'image ou aux intérêts de STECO. L'utilisation de la messagerie à titre privé ne doit ainsi en aucun cas engager la responsabilité de STECO. Afin de s'assurer du respect de ces règles, un dispositif de filtrage des messages par mots-clés pourra être mis en place à tout moment.

Les messages reçus depuis l'extérieur de l'entreprise sont contrôlés par un anti-virus avant d'être remis à l'utilisateur. L'accès aux liens, aux pièces jointes aux messages enregistrées sous certains formats (notamment de type .exe ou .vbs) est susceptible d'être empêché. Néanmoins, les messages reçus étant susceptibles de contenir des virus non détectés par l'anti-virus et s'activant par le simple affichage de ces messages dans le logiciel de gestion de la messagerie, l'ouverture automatique des messages reçus par le biais de l'« Aperçu » ou du « Volet de visualisation » est prohibée. Certains messages au contenu confidentiel pourront opportunément être cryptés pour des besoins exclusivement professionnels.

b. Utilisation personnelle de la messagerie

Dans le cadre professionnel, les messages envoyés étant signalés par la mention "Privé" ou "Perso" dans leur objet et étant classés dès l'envoi dans un dossier lui-même dénommé de la même façon relèvent du domaine privé conformément à la loi. Il en est de même concernant les messages reçus qui doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un support personnel pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

H. Contrôle de l'utilisation des Ressources informatiques

Dans le cadre de la maintenance de l'intégrité et de la cohérence des Ressources informatiques, les utilisations et usages de ces derniers sont consignés et peuvent être analysés dans le cadre de la réglementation.

L'utilisateur a le droit d'obtenir du DPO la confirmation que des données à caractère personnel le concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi qu'un certain nombre d'autres informations.

I. Informations et sanctions

La présente charte est publique et disponible sur le site internet de STECO.

Elle sera communiquée individuellement à chaque salarié, le cas échéant, par voie électronique dans la gestion documentaire. Le DPO sera à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d'information.

DocuSign Envelope ID: 3ACD6A8B-6F5E-4D30-8636-8E1DF0C3C351

La présente est transmise également aux sous-traitants en annexe du contrat.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la Gérance et le Responsable RGPD.

Si L'utilisateur met en œuvre des utilisations et/ou usages qui altèrent, directement ou indirectement, sciemment ou inconsciemment, l'intégrité et/ou la cohérence des Ressources Informatiques, il est susceptible d'engager sa responsabilité.

L'utilisation reconnue à des fins personnelles de certains services payants à travers les Ressources informatiques donnera également lieu à remboursement de la part de l'utilisateur concerné. Sa responsabilité étant également engagée, les mesures citées précédemment peuvent s'appliquer.

J. Entrée en vigueur et application

La présente Charte dites de sécurité de la donnée et sensibilisation RGPD régit l'utilisation des données, leur protection ainsi que les bonnes pratiques en matière de recours à la ressource informatique par tout utilisateur à compter de sa prise de connaissance.

La Charte s'applique lors de l'utilisation de Ressources informatiques et de traitement de la donnée personnelle.

K. Engagement de L'utilisateur

L'utilisateur reconnaît par la signature de la présente avoir pris connaissance de l'ensemble des obligations qui s'imposent à lui dans le cadre de l'utilisation des ressources ainsi que des Informations confidentielles auxquelles il aura accès au cours de l'exercice de sa mission.

Fait à Lagord, le 11 mars 2023

Pour la collectivité des Associés*

Frédéric MENOU

Président GROUPE STECO-HSF

DocuSigned by:
MENOU Frédéric
91D14EE176094D1...

**Validée par les associés lors de la réunion du 11/03/2023*