PROCÉDURE
POLITIQUE DE PROTECTION DES DONNÉES PERSONNEL

Écrit par : Dusty S.r.l.
Approuvé par : Administrateur unique
Faible niveau de confidentialité

Résumé

1. Portée, objet et destinataires

DUSTY S.r.l., ci-après dénommée "Entreprise / Société", s'engage à respecter les lois et les règlements
applicables relatives à la protection des données personnelles dans les pays où la Société opère. Cette politique énonce les principes de base avec lesquels la Société traite les données personnelles des

travailleurs des entreprises clientes, des clients, des fournisseurs, des partenaires
commerciaux, des employés et d'autres personnes et indique les responsabilités de leurs services d'entreprise et des employés lors du traitement des données personnelles.
Cette politique s'applique à la Société et aux sociétés qu'elle contrôle directement ou indirectement qui exercent des activités au sein de l'Espace économique européen (EEE) ou traitent des données personnelles de parties intéressées au sein de l'EEE.
Les destinataires de ce document sont tous les salariés, permanents ou temporaires, et tous les collaborateurs qui travaillent pour le compte de la Société.

2. Documents de référence
- Le RGPD UE 2016/679 (Règlement (UE) 2016/679 du Parlement européen et du Conseil
Du 27 avril 2016 concernant la protection des personnes physiques à l'égard des traitements
des données personnelles, ainsi que la libre circulation de ces données et abrogeant la directive 95/46/CE)
- Directives du Garant de la confidentialité pour la bonne application du RGPD
- Politique de protection des données personnelles des employés
- Politique de conservation des données
- Description du rôle du délégué à la protection des données
- Lignes directrices pour la liste des données et la cartographie des activités de traitement
- Procédure de demande d'accès aux données par la personne concernée
- Méthodologie d'évaluation de l'impact sur la protection des données
- Procédure de transfert transfrontalier de données personnelles
- Politiques de sécurité informatique
Procédure de rapport de violation de données

3. Définitions
Les définitions suivantes des termes utilisés dans le présent document sont tirées de l'article 4 du règlement sur la Protection générale des données de l'Union européenne (ou RGPD) :
Données personnelles : toute information concernant une personne physique identifiée ou identifiable ("Intéressé"); on considère la personne physique identifiable, directement ou
indirectement, en référence notamment à un identifiant tel que le nom, un certain nombre d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs éléments caractéristiques
de son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Données personnelles sensibles : Données personnelles qui, par leur nature, méritent une protection particulière, qui sont sensibles en termes de droits et libertés fondamentaux, puisque la
le contexte de leur traitement pourrait créer des risques importants pour les droits et les libertés fondamentaux.
Ces données personnelles devraient également inclure des données personnelles révélant l'origine raciale
ou ethniques, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, ainsi que
données génétiques, données biométriques destinées à identifier de manière unique une personne physique, données relatives à
la santé ou la vie sexuelle ou l'orientation sexuelle de la personne.
Responsable du traitement: (Contrôleur des données) La personne physique ou morale, l'autorité publique, le
service ou autre organisme qui, individuellement ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.
Sous-traitant: (Sous-traitant) une personne physique ou morale, une autorité publique,
le service ou tout autre organisme qui traite les données personnelles au nom du responsable du traitement.

Traitement : toute opération ou ensemble d'opérations, réalisée avec ou sans l'aide de procédés automatisés et appliqués aux données personnelles ou aux ensembles de données personnelles, telles que la collecte, l'enregistrement,
organisation, structuration, conservation, adaptation ou modification, extraction, la consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, comparaison ou interconnexion, restriction, suppression ou destruction.
Anonymisation : désidentification irréversible des données personnelles de telle sorte que la personne ne
peut être identifié en utilisant un temps, un coût et une technologie raisonnables par le contrôleur ou par
toute autre personne pour identifier la personne concernée. Les principes de protection des données ne devraient pas
s'appliquer donc aux informations anonymes, c'est-à-dire aux informations qui ne se réfèrent à aucune personne physique identifiée ou identifiable.
Pseudonymisation: le traitement des données personnelles de telle sorte que les données personnelles ne puissent pas être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelle visant à garantir que ces données personnelles ne sont pas attribuées à une personne physique identifiés ou identifiables. La pseudonymisation réduit, mais n'élimine pas complètement, la possibilité de lier les données personnelles à l'intéressé. Les données pseudonymisées étant néanmoins des données personnelles, leur traitement doit respecter les principes du Traitement des données personnelles.
Traitement transfrontalier : le traitement de données à caractère personnel qui a lieu dans le cadre des activités d'établissements dans plus d'un État membre d'un responsable du traitement ou d'un sous-traitant dans l'Union où le responsable du traitement ou le sous-traitant sont établis dans plus d'un État membre; ou le traitement des données qui a lieu dans le cadre des activités d'un seul établissement d'un responsable du traitement ou sous-traitant dans l'Union, mais qui affecte ou est susceptible d'affecter matériellement d'autres personnes concernées d'un État membre.
Autorité de surveillance : l'autorité publique indépendante établie par un État membre en vertu de l'Article 51 du RGPD de l'UE; pour l'Italie, il s'agit du Garant de la confidentialité.
Autorité de surveillance principale : L'autorité de surveillance ayant la responsabilité principale de gérer une activité de traitement de données transfrontalier, par exemple lorsqu'une personne concernée soumet une réclamation concernant le traitement de leurs données personnelles; elle est chargée, entre autres, de recevoir les notifications de violation des données, pour être informé des activités de traitement à risque et elle disposera d'autorité concernant ses fonctions pour assurer le respect des dispositions du RGPD de l'UE.

Chaque « **autorité de tutelle locale** » maintiendra toujours sur son propre territoire et contrôlera toute traitement local des données affectant les personnes concernées ou effectué par un responsable du traitement ou un sous-traitant à l'intérieur de l'Union ou à l'extérieur de l'Union si leur traitement est destiné aux parties intéressées résidant sur leur propre territoire. Leurs devoirs et pouvoirs comprennent l'enquête et l'exécution de mesures administratives et sanctions, la promotion de la sensibilisation du public aux risques, les règles, la sécurité et les droits relatifs au traitement des données personnelles, ainsi que l'accès à tout siège du responsable du traitement et du sous-traitant, y compris tous outils et moyens de traitement.
«**Etablissement principal à l'égard d'un responsable du traitement**» avec des établissements dans plus d'un État membre, le lieu de son administration centrale dans l'Union, à moins que les décisions sur les buts et les moyens des traitements de données à caractère personnel sont effectués dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir d'ordonner l'exécution de ces décisions, auquel cas l'établissement qui a pris de telles décisions est considéré comme l'établissement principal.
«**Établissement principal à l'égard d'un sous-traitant**»: Sous-traitant ayant des établissements

dans plus d'un État membre, le lieu de son administration centrale dans l'Union ou, si le responsable du traitement n'a pas d'administration centrale dans l'Union, l'établissement du responsable du traitement dans l'Union où sont effectuées les principales activités de traitement dans le contexte des activités d'un établissement du responsable du traitement dans la mesure où celui-ci est soumis à des obligations spécifiques en vertu du présent règlement.
«**Groupe entrepreneurial**»: un groupe constitué d'une société mère et de ses sociétés Chèque.

4. Principes applicables au traitement des données personnelles
Les principes applicables à la protection des données définissent les responsabilités des organisations dans la gestion des données personnelles. L'article 5 (2) du RGPD stipule que « le responsable du traitement est compétent pour se conformer aux principes, et en mesure de le prouver."

4.1 Légalité, équité et transparence
Les données personnelles sont traitées de manière licite, correcte et transparente vis-à-vis de l'intéressé.

4.2 Limitation des finalités
Les données personnelles sont collectées pour des finalités déterminées, explicites et légitimes, puis traitées de manière qui n'est pas incompatible avec ces finalités.

4.3 Minimisation des données
Les données personnelles sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. La société applique l'anonymisation ou la pseudonymisation des données personnelles, si possible, pour réduire le risque pour les personnes concernées.

4.4 Précision
Les données personnelles sont exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables sont prises pour supprimer ou rectifier rapidement les données inexactes au regard des finalités pour lesquelles elles sont traitées.

4.5 Limitation de la durée de conservation
Les données personnelles sont conservées pour une durée n'excédant pas la réalisation des finalités pour lesquelles sont traités.

4.6 Intégrité et confidentialité
Tenir compte des technologies disponibles et des autres mesures de sécurité, des coûts de mise en œuvre et de la probabilité et la gravité des risques sur les données personnelles, la Société met en œuvre des mesures techniques et organisationnelles pour assurer un niveau de sécurité adéquat pour les données personnelles, y compris la protection contre la destruction accidentelle ou illégale, le perte, modification, divulgation ou accès non autorisés.

4.7 Responsabilité
Les responsables du traitement sont compétents pour se conformer aux principes décrits ci-dessus et sont en mesure de le prouver.

5. Construire la protection des données dans les activités commerciales
Afin de démontrer le respect des principes de protection des données, une organisation doit créer protection des données dans ses activités commerciales.

5.1.Notification aux personnes concernées
(Voir la section 6 - Lignes directrices sur le traitement approprié - Point 1)

5.2 Choix et consentement de l'intéressé
(Voir la section 6 - Directives de traitement approprié - Point 2)

5.3 Collecte
La Société s'engage à collecter le moins de données personnelles possible. Si des données personnelles sont collectées auprès de tiers, le sous-traitant garantit que les données personnelles sont collectées légalement.

5.4 Utilisation, stockage et élimination
Les finalités, les modalités, la limite d'enregistrement et la durée de conservation des données personnelles sont conformes aux informations contenues dans la Politique de confidentialité. L'entreprise maintient l'exactitude, l'intégrité, la confidentialité et la pertinence des données personnelles en fonction de la finalité du traitement. L'entreprise utilise des mécanismes de sécurité conçus pour protéger les données personnelles afin d'empêcher qu'elles ne soient volées, utilisées d'une manière inappropriés ou abusés et elle empêche les violations de données personnelles. Le délégué à la protection des données est responsable du respect des 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 le traitement des données en son nom, le délégué à la protection des données s'assure que ce sous-traitant fournit des mesures de sécurité pour protéger les données personnelles appropriées aux risques associés. A cet effet, la Société utilise les Questionnaire de conformité du processeur RGPD. La Société exige contractuellement du fournisseur ou du partenaire commercial qu'il fournisse le même niveau de protection des données. Le fournisseur ou le partenaire commercial ne doit traiter les données personnelles que pour se conformer à ses obligations contractuelles envers la Société ou selon les instructions de la Société et non à d'autres fins.
Lorsque la Société traite des données personnelles conjointement avec un tiers indépendant, la Société précise explicitement leurs propres responsabilités et celles du tiers dans le contrat relatif ou tout autre document juridiquement contraignant, tel que l'accord avec le fournisseur de traitement des données.

5.6 Transfert transfrontalier de données personnelles
Avant de transférer des données personnelles de l'Espace économique européen (EEE), des mesures de protection adéquate doivent être utilisées, y compris la signature d'un accord de transfert de données, comme l'exige l'Union européenne et, si nécessaire, l'autorisation de l'autorité de protection des données compétente doit être obtenue. L'entité qui reçoit les données personnelles doit se conformer aux principes de traitement des données personnelles établis dans la procédure de transfert transfrontalier des données personnelles.

5.7 Droit d'accès des personnes concernées
Le délégué à la protection des données est chargé de fournir aux personnes concernées un mécanisme raisonnable d'accès pour leur permettre d'accéder à leurs données personnelles et leur permettre de mettre à jour, rectifier, supprimer ou transmettre leurs données personnelles. Le mécanisme d'accès sera détaillé dans la Procédure de demande d'accès aux données par la personne concernée.

5.8 Portabilité des données
Les personnes concernées ont le droit de recevoir, sur demande, une copie des données qu'elles nous

ont fournies dans un format structuré et de transmettre ces données à un autre responsable du traitement, gratuitement. Le chef de la protection des données est responsable de s'assurer que ces demandes sont traitées dans un délai d'un mois, qu'elles ne sont pas excessives et n'affectent pas les droits relatifs aux données personnelles d'autres personnes.

5.9 Droit à l'oubli
Sur demande, les intéressés ont le droit d'obtenir de la Société l'annulation de leurs données personnelles, lorsque ce droit n'est pas en contradiction avec d'autres législations (décret législatif 81/08 et modifications ultérieures). Lorsque la Société agit en tant que responsable du traitement, elle prend les mesures nécessaires (y compris les mesures techniques) pour informer les tiers qui utilisent ou traitent ces données pour répondre à la demande.

6. Directives de traitement appropriées
Les données personnelles ne doivent être traitées que si elles sont explicitement autorisées par le responsable du traitement.
La Société effectue l'évaluation d'impact sur la protection des données pour chaque activité de traitement des données en vertu des lignes directrices relatives à l'analyse d'impact sur la protection des données.

6.1 Communications aux intéressés
Au moment de la collecte ou avant de la collecte des données personnelles pour tout type d'activité de traitement, y compris, mais sans s'y limiter, la vente de produits, de services ou d'activités de marketing, le contrôleur de données a la responsabilité d'informer de manière adéquate les personnes concernées des éléments suivants: les types de données personnelles collectées, les finalités du traitement, les modalités de traitement, les droits des intéressés concernant leurs données personnelles, la période de conservation, les transferts internationaux potentiels de données, si les données seront partagées avec des tiers et les mesures de sécurité de la Société pour protéger les données personnelles. Ces informations sont fournies par une politique de confidentialité.
Lorsque des données personnelles sont partagées avec des tiers, le délégué à la protection des données doit s'assurer que les parties intéressées en ont été informées par le biais d'une politique de confidentialité.
Lorsque des données personnelles sont transférées vers un pays tiers dans le cadre de la politique de transfert transfrontalier des données, la politique de confidentialité doit refléter cela et indiquer clairement où et à qui les données personnelles des sujets sont transférées.
En cas de collecte de données personnelles sensibles, le délégué à la protection des données doit assurer que la politique de confidentialité indique explicitement le but pour lequel ces données personnelles sensibles sont collectés.

6.2.Obtenir le consentement
Chaque fois que le traitement des données personnelles est basé sur le consentement de l'intéressé, ou sur d'autres motifs légitimes, le délégué à la protection des données est chargé de conserver un enregistrement de ces consentement; il est également chargé de fournir aux personnes concernées la possibilité de donner leur consentement et doit les informer et s'assurer que leur consentement (chaque fois que le consentement est utilisé comme base légale pour le traitement) peut être révoqué à tout moment dans les limites permises par les lois en vigueur.
Lorsque la collecte de données personnelles concerne un mineur de moins de 16 ans, le Responsable du traitement des données garantit que le consentement du titulaire de la responsabilité parentale est fourni avant de la collecte à l'aide du formulaire de consentement du titulaire de la responsabilité parentale.
Lors d'une demande de rectification, de modification ou de destruction des enregistrements de données personnelles, le Responsable de la protection des données garantit que ces demandes sont

traitées dans un délai raisonnable, enregistre les demandes et garde une trace de celles-ci.
Les données personnelles ne sont traitées que pour les finalités pour lesquelles elles ont été initialement collectées. Dans le cas où la Société souhaite traiter les données personnelles collectées à d'autres fins, la Société requiert le consentement du concerné sous une forme écrite claire et concise. Une telle demande comprend l'objectif initial pour lequel des données et des finalités nouvelles ou supplémentaires ont été collectées. La demande comprend également le motif du changement de but. Le délégué à la protection des données est responsable du respect des règles en vigueur dans ce paragraphe.
Aujourd'hui et à l'avenir, le responsable du traitement et le délégué à la protection des données s'assurent que les méthodes de collecte sont conformes à la loi, aux bonnes pratiques et aux normes de l'industrie pertinente.
Le délégué à la protection des données est responsable de la création et de la tenue d'un registre de la Politique de confidentialité.

7. Organisation et responsabilité
La responsabilité d'assurer le bon traitement des données personnelles incombe à toute personne qui travaille pour ou avec la Société et a accès aux données personnelles traitées par la Société.
Les principaux domaines de responsabilité pour le traitement des données personnelles sont les rôles organisationnels suivants :

Administrateur unique : prend les décisions et approuve les stratégies générales de protection de la Société en ce qui concerne les données personnelles.

Le délégué à la protection des données : est responsable de la gestion du programme de protection des données personnelles et il est responsable du développement et de la promotion des politiques de protection des données personnelles du début à la fin, tel que défini dans la description du rôle du délégué à la protection des données.

Le **conseiller juridique**, en collaboration avec le **délégué à la protection des données**, surveille et analyse les lois sur les données et les changements réglementaires, élabore des exigences de conformité et aide les services de l'entreprise à la réalisation de leurs objectifs en matière de données personnelles.

Le responsable informatique est chargé de :
-S'assurer que tous les systèmes, services et équipements utilisés pour l'enregistrement des données sont satisfaisants les normes de sécurité acceptables.
-Effectue des contrôles et des analyses réguliers pour vous assurer que votre matériel et vos logiciels sont sûrs et travaillent correctement.

Le service communication est chargé de :
-Approuver toutes les déclarations de protection des données jointes aux communications telles que les e-mails et les lettres.
-Répondre à toute question sur la protection des données des journalistes ou des médias tels que les journaux.
-Si nécessaire, collaborer avec le délégué à la protection des données pour s'assurer que les initiatives de marketing respectent les principes de la protection des données.

Le responsable des ressources humaines est chargé de :
-Améliorer la sensibilisation de tous les employés sur la protection des données personnelles des utilisateurs.
-Organiser des formations de compétence et de sensibilisation à la protection des données personnelles pour les employés qui travaillent avec des données personnelles.

-Protéger les données personnelles des employés du début à la fin. Il garantit que les données personnelles des employés sont traités sur la base des objectifs commerciaux légitimes et des besoins de l'employeur.

Le responsable des achats est responsable du transfert des responsabilités en matière de protection des données aux fournisseurs et l'amélioration du niveau de sensibilisation des fournisseurs à la protection des données personnelles, ainsi que le flux descendant de données personnelles demandées à tout fournisseur tiers qui l'entreprise utilise. Le service Achats doit s'assurer que la Société se réserve le droit d'effectuer un audit aux fournisseurs.

8. Lignes directrices pour l'établissement de l'autorité de surveillance principale
La Société n'est actuellement pas en mesure d'appliquer les dispositions du point 8 ; au cas où elle se trouve dans ces conditions, elle appliquera la règle décrite ci-dessous.

8.1 Nécessité d'établir l'autorité de surveillance principale
L'identification d'une autorité de contrôle principale n'est nécessaire que si l'entreprise effectue le traitement des données personnelles transfrontalières.
Un traitement transfrontalier de données à caractère personnel a lieu si :
a) Le traitement des données personnelles est effectué par des sociétés contrôlées par la Société établies dans d'autres États Membres; ou alors
b) le traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un seul établissement d'une entreprise dans l'Union, mais qui affecte ou affecte probablement substantiellement plus de parties intéressées d'un État membre.
Si la Société n'a d'établissements que dans un seul État membre et ses activités de traitement ne concernent que les intéressés par cet État membre, il n'est pas nécessaire de créer une autorité de surveillance chef de file. La seule autorité compétente sera l'autorité de contrôle du pays où la société qui est légalement établie.

8.2 L'usine principale et l'autorité de surveillance principale
8.2.1. L'établissement principal du responsable du traitement
L'Administrateur de la Société doit identifier l'établissement principal afin qu'il puisse être déterminer l'autorité de contrôle principale.
Si la Société est établie dans un État membre de l'Union et prend des décisions relatives aux activités de traitement au lieu de son administration centrale, il y aura une seule autorité de contrôle chef de file pour les activités de traitement de données effectuées par la Société.
Si la Société dispose de plusieurs établissements qui agissent de manière indépendante et prennent des décisions sur les finalités et les moyens de traitement des données personnelles, la haute direction de la Société doit reconnaître qu'il y a plus d'une autorité de contrôle principale.

8.2.2. L'établissement principal du sous-traitant
Dans le cas où la Société agit en tant que processeur de données, l'usine principale sera le siège social de l'administration centrale. Si le poste de l'administration centrale n'est pas situé dans l'UE, l'établissement principal sera l'établissement dans l'UE où se déroulent les principales activités de transformation.

8.2.3. L'Etablissement Principal pour les Entreprises hors Union pour les Responsables de Traitement et Sous-Traitants
Si la Société n'a pas d'établissement principal dans l'Union et a une ou plusieurs filiales dans l'UE, alors l'autorité de contrôle compétente est l'autorité de contrôle locale. Si la Société n'a pas d'établissement principal dans l'Union ou de filiales dans l'UE, elle doit désigner un représentant dans l'UE et l'autorité de contrôle compétente sera l'autorité de contrôle locale où le représentant se trouve.

9. Réponse aux incidents de violation de données personnelles
Lorsque la Société a connaissance d'une violation présumée ou réelle des données personnelles, le Gestionnaire de la protection des données mène une enquête interne et prend les mesures correctives appropriées en temps opportun, conformément à la politique de violation des données. Lorsqu'il existe des risques pour les droits et les libertés des intéressés, la Société informe l'autorité de contrôle chargée de la protection des données sans retards injustifiés et, si possible, dans les 72 heures.

10. Audit et responsabilité
Le délégué à la protection des données est chargé de vérifier comment les services de l'entreprise mettre en œuvre cette politique.
Tout employé qui enfreint cette politique sera soumis à des mesures disciplinaires et peut même être exposé à une responsabilité civile ou pénale si sa conduite enfreint les lois ou les règlements.

11. Conflits avec la loi
Cette politique est destinée à se conformer aux lois et aux règlements du lieu d'établissement et des pays dans lesquels DUSTY S.r.l. opère. En cas de conflit entre la présente Politique et les lois et les règlements applicables, ceux-ci prévaudront ceux derniers.

12. Gestion des inscriptions sur la base de ce document

Nom de document	**Lieu d'archivage**	**Personne responsable d'archivage**	**Chèques pour la protection du document**	**Temps d'archivage**
Formulaire de Consentement de l'intéressé	Serveur de l'Entreprise Dossier RGPD DUSTY	Directeur de la protection des données	Seulement de personnes autorisées peuvent avoir accès aux modules	10 ans
Formulaire de rétractation de l'intéressé	Serveur de l'Entreprise Dossier RGPD DUSTY	Directeur de la protection des données	Seulement de personnes autorisées peuvent avoir accès aux modules	10 ans
Formulaire de Consentement des Titulaires de la Responsabilité Parentale	Serveur de l'Entreprise Dossier RGPD DUSTY	Directeur de la protection des données	Seulement de personnes autorisées peuvent avoir accès aux modules	10 ans
Formulaire de rétractation des Titulaires de la Responsabilité Parentale	Serveur de l'Entreprise Dossier RGPD DUSTY	Directeur de la protection des données	Seulement de personnes autorisées peuvent avoir accès aux modules	10 ans
Accords avec les fournisseurs du	Serveur de l'Entreprise	Directeur de la protection des	Seulement de personnes	5 ans après la expiration du

Traitement des Données	Dossier RGPD DUSTY	données	autorisées peuvent avoir accès au dossiers	Contrat
Registre des Informations sur la Confidentialité	Serveur de l'Entreprise Dossier RGPD DUSTY	Directeur de la protection des données	Seulement de personnes autorisées peuvent avoir accès aux modules	Permanent

13. Validité et gestion du document

Ce document est effectif à partir du 11/02/2019.

La personne responsable de ce document est le contrôleur des données, qui nomme le gestionnaire de la protection des données pour vérifier et, si nécessaire, mettre à jour le document de manière annuel.