MS INDUSTRIE
Ingénierie Machines Spéciales

Charte de traitement des données

Version 2	Date de diffusion : 04/05/2026
Nb de pages : 5	Rédigé par : Manuel COLASSE

1. Introduction

L'entreprise s'engage à respecter la confidentialité et la sécurité des données personnelles de ses collaborateurs, clients, fournisseurs, et partenaires, conformément aux dispositions du Règlement Général sur la Protection des Données (RGPD) et à la législation en vigueur. Cette charte a pour objectif de définir les principes de collecte, de traitement, de conservation, et de gestion des données personnelles, en précisant les délais légaux de conservation et les responsabilités des collaborateurs.

---

2. Objectifs de cette charte

Cette charte a pour objectif de :

- Assurer une gestion transparente, sécurisée et conforme des données personnelles,
- Sensibiliser les collaborateurs sur leurs responsabilités concernant le traitement des données,
- Préciser les durées légales de conservation des données en fonction de leur nature.

---

3. Types de données personnelles collectées

L'entreprise collecte et traite diverses catégories de données personnelles, selon les activités suivantes :

- Données des collaborateurs : Nom, prénom, adresse, numéro de sécurité sociale, données bancaires, informations relatives à la paie, formations suivies, évaluations professionnelles, etc.
- Données des clients et prospects : Nom, prénom, adresse, coordonnées professionnelles, historique des commandes, préférences produits, images et visuels transmis.
- Données des fournisseurs et partenaires : Informations de contact, historique des transactions, données financières nécessaires au paiement.

---

4. Principes de traitement des données

Les données personnelles sont collectées et traitées dans le respect des principes énoncés par le RGPD :

- Licéité, loyauté et transparence
- Limitation des finalités
- Minimisation des données
- Exactitude
- Conservation limitée
- Sécurité et confidentialité des données

---

5. Durée de conservation des données

Les données personnelles doivent être conservées pendant une période n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été collectées. En fonction des types de données et des catégories de personnes concernées, les délais de conservation sont définis comme suit :

1. Données des collaborateurs :
   - Documents liés à l'embauche (contrats de travail, informations personnelles) : Pendant toute la durée de la relation de travail et 5 ans après la fin du contrat (selon l'Article L1234-19 du Code du travail).
   - Données liées à la paie (bulletins de salaire, déclarations sociales) : 5 ans à partir de la fin de l'année civile concernée (Article L3243-4 du Code du travail).
   - Évaluations professionnelles et formations : Pendant 5 ans après la fin de la relation de travail.
   - Données de santé (si collectées) : Conformément aux règles spécifiques de confidentialité, elles sont conservées pendant la durée nécessaire à leur traitement, mais en aucun cas plus de 10 ans.
2. Données des clients et prospects :
   - Informations relatives aux commandes et contrats : 5 ans après la fin de la relation commerciale (Article L110-4 du Code de commerce).
   - Données de prospection commerciale (coordonnées et préférences) : Pendant 3 ans à compter du dernier contact avec le prospect, sauf opposition ou retrait de consentement.
3. Données des fournisseurs et partenaires :
   - Documents contractuels et informations financières : 5 ans après la fin de la relation contractuelle.
   - Données de gestion des commandes et paiements : 5 ans à compter de la dernière transaction.
4. Données liées à des obligations légales : Certaines données doivent être conservées plus longtemps en raison d'obligations légales spécifiques, telles que les obligations fiscales, comptables, ou de sécurité sociale. Par exemple :
   - Comptabilité et facturation : 10 ans à partir de la clôture de l'exercice fiscal concerné (Article L123-22 du Code de commerce).

- Documents liés à des litiges ou des contentieux : Ils peuvent être conservés pendant la durée nécessaire à la gestion du contentieux, avec un délai maximal de 5 ans après la clôture de l'affaire.

---

6. Responsabilités des collaborateurs

Chaque collaborateur doit :

- Respecter les procédures de gestion des données personnelles définies par l'entreprise.
- S'assurer que seules les données nécessaires à l'activité professionnelle sont collectées et traitées.
- Garantir la confidentialité des données, en particulier lors de l'accès, du stockage, du traitement, et de la transmission de celles-ci.
- Suivre les formations régulières proposées par l'entreprise concernant le traitement des données et la sécurité.

---

7. Sécurité des données

L'entreprise met en œuvre des mesures techniques et organisationnelles pour protéger les données personnelles contre toute perte, altération, divulgation ou accès non autorisé. Ces mesures incluent :

- Contrôle des accès : Accès restreint aux données sensibles.
- Sauvegardes régulières : Sauvegarde sécurisée des données essentielles.
- Formation continue : Sessions de sensibilisation à la protection des données.

---

8. Droit des personnes concernées

Conformément au RGPD, toute personne concernée par le traitement de ses données dispose des droits suivants :

- Droit d'accès : Demander la consultation de ses données personnelles.
- Droit de rectification : Corriger des données inexactes ou incomplètes.
- Droit à l'effacement : Demander l'effacement des données sous certaines conditions.
- Droit à la limitation du traitement : Suspendre temporairement le traitement des données.
- Droit d'opposition : S'opposer au traitement des données pour des raisons légitimes.

---

9. Partage et transfert des données

- Les données personnelles peuvent être partagées avec des tiers dans le cadre de la gestion de la relation contractuelle, pour respecter des obligations légales ou avec des prestataires de services. Les données ne seront jamais transférées en dehors de l'Union Européenne sans garanties adéquates.
- Partage interne : Les données ne sont accessibles qu'aux collaborateurs ayant un besoin légitime d'y accéder.

---

10. Sanctions en cas de non-respect

Tout non-respect des obligations définies par cette charte pourra entraîner des sanctions disciplinaires, pouvant aller jusqu'à un licenciement en cas de violation grave des règles. Des sanctions pénales peuvent également être applicables en cas de non-respect des obligations légales de protection des données (amendes ou poursuites judiciaires).

---

11. Suivi et mise à jour de la charte

Cette charte est régulièrement mise à jour pour garantir sa conformité avec les évolutions législatives et les meilleures pratiques en matière de protection des données. Toute mise à jour sera communiquée à l'ensemble des collaborateurs.

---

12. Conclusion

La protection des données personnelles est essentielle pour maintenir la confiance de nos collaborateurs, clients et partenaires. L'ensemble des collaborateurs est responsable de la sécurité des données et doit respecter cette charte pour garantir la conformité avec le RGPD et les règles internes de l'entreprise.

Cette charte fera l'objet d'une revue annuelle.

Procédure d'alerte en cas de problème de sécurité de l'information

Objectif

Cette procédure permet de signaler rapidement tout problème ou incident lié à la sécurité des informations pour assurer leur protection.

Quand signaler un incident ?

Signalez toute situation suspecte ou tout incident affectant la sécurité des informations, comme :

- Accès non autorisé à des données sensibles.
- Perte ou vol de matériel (ordinateur, téléphone, etc.).
- Suspicion de cyberattaque (phishing, ransomware, etc.).

Comment signaler un incident ?

1. Par email : Envoyer un message à qualité@ms-industrie.com avec une description de l'incident (qu'est-ce qui s'est passé, quand, où, qui est concerné ?).
2. Par téléphone : Contacter immédiatement la direction si l'incident est urgent.

Que faire après l'alerte ?

- Réception de l'alerte : La direction accuse réception dans les 24 heures.
- Analyse : La direction évalue la gravité et prend les mesures nécessaires pour limiter les risques.
- Suivi : Vous serez informé des actions entreprises et des résultats de l'analyse après la résolution.

Confidentialité

Les alertes sont traitées de manière confidentielle, et aucune sanction ne sera appliquée pour avoir signalé un incident.