

MANUEL DE CONFORMITÉ RGPD

Chapitre 1 : Présentation de l'entreprise et du cadre RGPD

CHAPITRE 2 – Politique de confidentialité

CHAPITRE 3 – Registre des traitements

CHAPITRE 4 – Politique de conservation et d'archivage des données

CHAPITRE 5 – Politique de sécurité des systèmes d'information

CHAPITRE 6 – Gestion des violations de données personnelles

CHAPITRE 7 – Procédure d'exercice des droits des personnes

CHAPITRE 8 – Registres internes RGPD

CHAPITRE 9 – Charte de confidentialité des salariés et collaborateurs

CHAPITRE 10 – Engagement de confidentialité

CHAPITRE 11 – Synthèse du dispositif RGPD

Chapitre 1 : Présentation de l'entreprise et du cadre RGPD

1. Présentation de l'entreprise

1.1 Identification

Raison sociale : Scierie Ehrstein

Activité : Exploitation d'une scierie et transformation du bois.

Adresse :

2, rue de la Sauer
67510 Lembach
France

SIRET : 618 502 132 00011

Site internet : www.scierie-ehrstein.com

Adresse électronique : info@scierie-ehrstein.com

1.2 Direction

La direction de l'entreprise est assurée par :

- Laurent Ehrstein
- Jacky Ehrstein
- Elise Ehrstein

Ils sont responsables de la mise en œuvre des mesures nécessaires afin d'assurer la conformité de l'entreprise au Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) ainsi qu'à la législation française applicable.

1.3 Objet du présent manuel

Le présent manuel a pour objectif de définir les règles appliquées par Scierie Ehrstein concernant :

- la collecte des données personnelles ;
- leur utilisation ;
- leur conservation ;

- leur sécurisation ;
- les droits des personnes concernées ;
- les procédures internes de conformité.

Il constitue le document de référence utilisé par l'entreprise pour démontrer sa conformité au RGPD.

2. Champ d'application

Le présent manuel s'applique à l'ensemble des traitements de données personnelles réalisés par Scierie Ehrstein dans le cadre de son activité professionnelle.

Sont notamment concernés :

- les prospects ;
- les clients ;
- les fournisseurs ;
- les transporteurs ;
- les partenaires commerciaux ;
- les visiteurs du site internet ;
- les salariés et collaborateurs.

3. Définitions

Au sens du RGPD :

Donnée personnelle

Toute information permettant d'identifier directement ou indirectement une personne physique.

Exemples :

- nom ;
- prénom ;
- adresse postale ;
- adresse électronique ;
- numéro de téléphone.

Traitement

Toute opération réalisée sur des données personnelles :

- collecte ;
- consultation ;
- enregistrement ;
- modification ;
- conservation ;
- suppression.

Responsable du traitement

La Scierie Ehrstein détermine les finalités et les moyens des traitements réalisés dans le cadre de son activité.

Sous-traitant

Toute société traitant des données pour le compte de Scierie Ehrstein.

Exemples :

- hébergeur du site internet (OVH) ;
- Microsoft 365 ;
- prestataires informatiques

4. Principes appliqués

Scierie Ehrstein s'engage à respecter les principes suivants :

Licéité

Les données sont collectées uniquement lorsqu'une base juridique existe.

Transparence

Les personnes sont informées de la manière dont leurs données sont utilisées.

Minimisation

Seules les données strictement nécessaires sont collectées.

Exactitude

Les informations sont mises à jour lorsque cela est nécessaire.

Limitation de conservation

Les données ne sont pas conservées plus longtemps que nécessaire, sauf obligation légale.

Intégrité et confidentialité

Des mesures techniques et organisationnelles protègent les données contre toute utilisation non autorisée.

Responsabilité

Scierie Ehrstein documente ses traitements et est en mesure de démontrer sa conformité à tout moment.

5. Organisation de la conformité

La direction veille notamment à :

- sensibiliser les collaborateurs aux règles de protection des données ;
- sécuriser les postes informatiques ;
- maintenir les sauvegardes hebdomadaires ;
- contrôler les accès au NAS de l'entreprise ;
- limiter les accès aux seules personnes autorisées ;
- mettre à jour les procédures lorsque la réglementation évolue.

Chaque collaborateur manipulant des données personnelles est tenu de respecter les dispositions du présent manuel.

CHAPITRE 2 – Politique de confidentialité

1. Objet

La présente politique de confidentialité a pour objet d'informer les utilisateurs du site www.scierie-ehrstein.com sur la manière dont la Scierie Ehrstein collecte, utilise, protège et conserve leurs données personnelles, conformément au Règlement (UE) 2016/679 (RGPD) et à la législation française en vigueur.

2. Responsable du traitement

Le responsable du traitement est :

Scierie Ehrstein
2, rue de la Sauer
67510 Lembach – France

SIRET : **618 502 132 00011**

Adresse de contact : info@scierie-ehrstein.com

3. Données collectées

Selon les échanges avec l'entreprise, les données suivantes peuvent être collectées :

- Nom et prénom
- Adresse postale
- Adresse électronique
- Numéro de téléphone
- Informations nécessaires à l'établissement d'un devis ou d'une commande
- Informations de facturation

Aucune donnée dite « sensible » au sens du RGPD n'est demandée.

4. Finalités des traitements

Les données sont collectées afin de :

- répondre aux demandes effectuées via le formulaire de contact ;
- établir des devis ;
- traiter les commandes ;
- assurer le suivi des livraisons ;
- établir les factures ;
- assurer le service après-vente ;
- répondre aux obligations comptables, fiscales et légales.

Les données ne sont utilisées à aucune autre fin incompatible avec celles décrites ci-dessus.

5. Base juridique

Les traitements reposent sur :

- l'exécution de mesures précontractuelles (demande de devis) ;
- l'exécution d'un contrat (commande, livraison, facturation) ;
- le respect des obligations légales (comptabilité, fiscalité) ;
- l'intérêt légitime de la Scierie Ehrstein pour assurer la gestion de sa clientèle.

6. Destinataires des données

Les données personnelles sont accessibles uniquement :

- aux gérants de la Scierie Ehrstein ;
- aux collaborateurs autorisés lorsque cela est nécessaire ;

- aux prestataires techniques intervenant pour le fonctionnement des services (hébergement, maintenance informatique, services Microsoft 365) ;
- aux autorités administratives ou judiciaires lorsque la loi l'impose.

Les données ne sont ni vendues ni cédées à des fins commerciales.

7. Hébergement et sécurité

Le site internet est hébergé chez OVH.

Les données de gestion commerciale sont conservées sur un serveur NAS situé dans les locaux de l'entreprise, protégé par un mot de passe. Des sauvegardes hebdomadaires sont réalisées afin d'assurer la continuité d'activité en cas d'incident.

L'entreprise met en œuvre des mesures techniques et organisationnelles destinées à protéger les données contre tout accès non autorisé, perte, destruction ou divulgation.

8. Durée de conservation

Les données sont conservées selon les durées suivantes :

Catégorie	Durée
Demandes de contact	3 ans après le dernier échange
Devis non acceptés	3 ans
Clients	Pendant la relation commerciale puis archivage selon les obligations légales
Factures et documents comptables	10 ans
Correspondances administratives	Selon les délais légaux applicables

À l'expiration de ces délais, les données sont supprimées ou archivées lorsque la loi l'exige.

9. Vos droits

Conformément au RGPD, toute personne dispose des droits suivants :

- droit d'accès ;
- droit de rectification ;
- droit à l'effacement lorsque les conditions légales sont réunies ;
- droit à la limitation du traitement ;
- droit d'opposition ;
- droit à la portabilité lorsque celui-ci est applicable.

Toute demande peut être adressée à :

info@scierie-ehrstein.com

Une réponse sera apportée dans un délai maximal d'un mois, sauf cas particuliers prévus par la réglementation.

10. Réclamation

Si une personne estime que ses droits ne sont pas respectés, elle peut adresser une réclamation à la Commission Nationale de l'Informatique et des Libertés (CNIL).

11. Cookies

Le site utilise uniquement les cookies nécessaires à son fonctionnement, ainsi que les cookies éventuellement acceptés par l'utilisateur via le bandeau de gestion des cookies.

Aucun outil de mesure d'audience tel que Google Analytics n'est utilisé à ce jour.

12. Modification de la politique

La présente politique peut être modifiée afin de tenir compte des évolutions législatives, réglementaires ou techniques.

La version publiée sur le site internet est la version en vigueur.

CHAPITRE 3 – Registre des traitements

1. Objet

Le présent registre est établi conformément à l'article 30 du Règlement (UE) 2016/679 (RGPD).

Il recense l'ensemble des traitements de données personnelles réalisés par la Scierie Ehrstein dans le cadre de son activité.

Responsable du traitement :

Scierie Ehrstein
2, rue de la Sauer
67510 Lembach

Traitement n°1 – Gestion des demandes de contact

Finalité

Répondre aux demandes adressées via le formulaire de contact du site internet ou par courrier électronique.

Personnes concernées

- Prospects
- Clients

Données traitées

- Nom
- Adresse e-mail
- Téléphone
- Contenu du message

Base juridique

Mesures précontractuelles à la demande de la personne concernée.

Destinataires

- Gérants
- Personnel administratif autorisé

Support

- Microsoft 365
- NAS interne

Durée de conservation

3 ans après le dernier contact.

Mesures de sécurité

- Accès sécurisé par mot de passe
- Comptes Microsoft protégés
- Sauvegarde hebdomadaire
- Accès limité aux personnes autorisées
-

Traitement n°2 – Établissement des devis

Finalité

Préparer et transmettre les devis aux clients.

Personnes concernées

- Prospects
- Clients

Données traitées

- Nom
- Adresse
- Téléphone
- Adresse e-mail
- Informations nécessaires au devis

Base juridique

Mesures précontractuelles.

Destinataires

Personnel administratif habilité.

Support

- Logiciel ANT
- Microsoft 365
- NAS

Durée

3 ans si le devis n'est pas accepté.

Si le devis est accepté, les données sont intégrées au dossier client.

Traitement n°3 – Gestion des commandes

Finalité

Traiter les commandes de bois et assurer leur suivi.

Données

- Identité

- Coordonnées
- Adresse de livraison
- Historique des commandes

Base juridique

Exécution du contrat.

Destinataires

- Direction
- Personnel administratif
- Personnel chargé de la préparation des commandes lorsque cela est nécessaire

Conservation

Pendant la relation commerciale.

Archivage ensuite selon les obligations légales.

Traitement n°4 – Facturation

Finalité

Établir les factures et assurer le suivi comptable.

Données

- Nom
- Adresse
- Coordonnées
- Informations de facturation
- Historique des achats

Logiciels

- ANT
- Microsoft 365

Base juridique

Obligation légale.

Conservation

10 ans conformément au Code de commerce.

Traitement n°5 – Gestion des fournisseurs**Finalité**

Gestion administrative des fournisseurs.

Données

- Nom du contact
- Fonction
- Téléphone
- Adresse e-mail professionnelle
- Coordonnées de l'entreprise

Base juridique

Exécution des contrats.

Conservation

Durée de la relation commerciale puis archivage légal.

Traitement n°6 – Gestion des e-mails**Finalité**

Gestion de la correspondance professionnelle.

Données

- Adresse e-mail
- Nom
- Téléphone
- Pièces jointes
- Historique des échanges

Outil

Microsoft 365

Conservation

Pendant la durée nécessaire au traitement des échanges, puis archivage lorsqu'ils concernent une commande ou une obligation légale.

Traitement n°7 – Sauvegardes informatiques

Finalité

Garantir la restauration des données en cas de panne, de perte ou d'incident.

Données concernées

Toutes les données professionnelles stockées sur les systèmes de l'entreprise.

Support

NAS sécurisé.

Sauvegardes

Hebdomadaires.

Accès

Réservé aux gérants et aux personnes habilitées.

Traitement n°8 – Gestion des droits RGPD

Finalité

Traiter les demandes d'accès, de rectification, d'effacement, de limitation, d'opposition ou de portabilité.

Données

- Identité du demandeur
- Coordonnées
- Nature de la demande
- Date de traitement

Base juridique

Obligation légale.

Conservation

3 ans après la clôture de la demande.

Sous-traitants

Les principaux sous-traitants identifiés sont :

Prestataire**Finalité**

OVH

Hébergement du site internet

Microsoft

Messagerie et services Microsoft 365

Prestataire informatique (si applicable) Maintenance informatique

Chaque sous-traitant est tenu de présenter des garanties suffisantes en matière de protection des données personnelles.

Transferts hors Union européenne

À la connaissance de la Scierie Ehrstein, aucun transfert volontaire de données personnelles vers un pays tiers n'est réalisé en dehors des services utilisés dans Microsoft 365, lesquels sont encadrés par les mécanismes de conformité prévus par la réglementation applicable.

Mise à jour du registre

Le présent registre est mis à jour :

- lors de la création d'un nouveau traitement ;
- lors de la suppression d'un traitement ;
- lors de toute évolution importante des outils ou des finalités.

La direction est responsable de son maintien à jour.

CHAPITRE 4 – Politique de conservation et d'archivage des données

1. Objet

La présente politique définit les règles de conservation, d'archivage et de suppression des données personnelles traitées par la Scierie Ehrstein.

Elle s'applique à l'ensemble des données collectées dans le cadre de l'activité de l'entreprise.

2. Principes généraux

La Scierie Ehrstein applique les principes suivants :

- ne collecter que les données nécessaires à son activité ;
- conserver les données uniquement pendant une durée justifiée ;

- archiver les documents lorsque la loi l'impose ;
- supprimer les données devenues inutiles ;
- protéger les données durant toute leur durée de conservation.

3. Tableau des durées de conservation

Traitement	Durée de conservation	Justification
Formulaire de contact	3 ans après le dernier échange	Gestion des prospects
Demande de devis non acceptée	3 ans	Relation commerciale
Devis accepté	Intégré au dossier client	Exécution du contrat
Données clients	Durée de la relation commerciale	Gestion des commandes
Factures	10 ans	Obligations comptables et fiscales
Pièces comptables	10 ans	Code de commerce
Courriers électroniques liés à une commande	Durée de la relation commerciale puis archivage si nécessaire	Suivi commercial
Contrats fournisseurs	Durée du contrat puis archivage légal	Gestion administrative
Sauvegardes	Rotation hebdomadaire selon la politique de sauvegarde	Continuité d'activité
Registre RGPD	Mise à jour permanente	Obligation réglementaire
Registre des violations	5 ans	Traçabilité
Registre des demandes RGPD	3 ans	Justification des traitements

4. Archivage

Lorsque les données ne sont plus utilisées au quotidien mais doivent être conservées pour répondre à une obligation légale, elles sont placées en archivage.

L'archivage est réservé aux personnes autorisées.

Les données archivées ne sont consultées qu'en cas de nécessité administrative, comptable, fiscale ou judiciaire.

5. Suppression des données

À l'expiration de la durée de conservation applicable :

- les données sont supprimées ;
- ou rendues anonymes lorsque cela est possible ;
- ou archivées uniquement lorsqu'une obligation légale l'impose.

La suppression concerne également les copies devenues inutiles.

6. Sauvegardes

La Scierie Ehrstein réalise des sauvegardes hebdomadaires de ses données professionnelles.

Les sauvegardes ont pour objectif :

- la restauration après incident ;
- la protection contre la perte de données ;
- la continuité de l'activité.

Les sauvegardes ne constituent pas un moyen de prolonger la durée de conservation des données personnelles.

Lorsqu'une donnée est supprimée conformément à la présente politique, elle disparaît également des sauvegardes selon leur cycle normal de rotation.

7. Sécurisation des données conservées

Les données sont stockées :

- sur un NAS interne sécurisé par authentification ;
- dans les services Microsoft 365 utilisés par l'entreprise ;
- dans le logiciel de gestion et de facturation ANT.

Les mesures de protection comprennent notamment :

- contrôle des accès ;
- mots de passe individuels ;
- mises à jour régulières des systèmes ;
- sauvegardes hebdomadaires ;
- protection contre les logiciels malveillants.

8. Responsabilités

Les gérants de la Scierie Ehrstein veillent à :

- l'application de la présente politique ;
- la suppression régulière des données devenues inutiles ;
- la mise à jour des durées de conservation lorsque la réglementation évolue.

Les collaborateurs ayant accès aux données sont tenus de respecter ces règles.

9. Révision de la politique

La présente politique est révisée :

- lors d'une évolution réglementaire ;
- lors d'un changement d'organisation ;
- lors de la mise en œuvre d'un nouveau traitement de données ;
- au minimum tous les deux ans.

Toute modification est validée par la direction avant sa mise en application.

CHAPITRE 5 – Politique de sécurité des systèmes d'information

1. Objet

La présente politique définit les mesures techniques et organisationnelles mises en place par la Scierie Ehrstein afin d'assurer la sécurité, l'intégrité et la confidentialité des données personnelles traitées dans le cadre de son activité.

Elle est conforme aux exigences de l'article 32 du Règlement (UE) 2016/679 (RGPD).

2. Principes de sécurité

La Scierie Ehrstein applique les principes suivants :

- protection des données contre tout accès non autorisé ;
- limitation des accès aux seules personnes habilitées ;
- sécurisation des équipements informatiques ;
- sauvegarde régulière des données ;
- prévention des pertes de données ;
- traçabilité des opérations importantes.

3. Gestion des accès

L'accès aux données est strictement encadré :

- chaque utilisateur dispose d'un compte nominatif ;
- les accès sont limités en fonction des besoins professionnels ;
- les mots de passe sont personnels et confidentiels ;
- les accès sont révoqués immédiatement en cas de départ d'un collaborateur.

Les accès aux données sont principalement réalisés via :

- Microsoft 365 (messagerie et documents) ;
- logiciel de gestion et facturation ANT ;
- serveur NAS interne.

4. Politique de mots de passe

Les mots de passe doivent respecter les règles suivantes :

- longueur minimale recommandée : 8 caractères ;
- combinaison de lettres, chiffres et caractères spéciaux ;
- interdiction d'utiliser des mots de passe simples ou réutilisés ;
- modification en cas de suspicion de compromission.

L'authentification multifacteur (MFA) est recommandée, notamment pour les comptes Microsoft 365.

5. Sécurité des équipements

Les équipements utilisés au sein de l'entreprise sont protégés par :

- antivirus et protections contre les logiciels malveillants ;
- mises à jour régulières des systèmes ;

- verrouillage automatique des postes ;
- accès limité aux utilisateurs autorisés.

Les postes informatiques utilisés pour accéder aux données professionnelles ne doivent pas être partagés sans contrôle des accès.

6. Sécurité du NAS (serveur local)

Les données de l'entreprise sont stockées sur un NAS interne.

Les mesures de sécurité comprennent :

- protection par mot de passe ;
- accès restreint aux gérants et personnels autorisés ;
- sauvegardes hebdomadaires ;
- contrôle des accès réseau ;
- stockage dans les locaux de l'entreprise.

7. Sauvegardes

Des sauvegardes hebdomadaires sont réalisées afin d'assurer la continuité d'activité.

Elles permettent :

- la restauration des données en cas de panne ;
- la protection contre les erreurs humaines ;
- la reprise d'activité après incident.

Les sauvegardes sont conservées pour une durée définie selon les besoins de restauration et ne doivent pas être utilisées comme stockage permanent.

8. Sécurité des services cloud (Microsoft 365)

L'entreprise utilise Microsoft 365 pour la messagerie et le stockage de documents.

Les mesures de sécurité incluent :

- authentification sécurisée ;
- chiffrement des communications ;
- contrôle des accès ;
- gestion des permissions par utilisateur ;
- supervision des connexions.

9. Sécurité du site internet

Le site www.scierie-ehrstein.com est hébergé chez OVH.

Les mesures de sécurité comprennent :

- infrastructure sécurisée de l'hébergeur ;
- certificats SSL pour les échanges sécurisés (HTTPS) ;
- protection contre les attaques courantes ;
- mises à jour techniques selon les besoins.

10. Gestion des incidents de sécurité

En cas d'incident (perte de données, accès non autorisé, attaque informatique), la procédure suivante est appliquée :

1. Identification de l'incident ;
2. Containment (limitation de l'impact) ;
3. Analyse de la cause ;
4. Restauration des données via sauvegarde si nécessaire ;
5. Notification à la direction ;
6. Évaluation de l'obligation de notification à la CNIL dans les 72 heures si nécessaire.

11. Sensibilisation du personnel

Les personnes ayant accès aux données sont sensibilisées aux bonnes pratiques :

- vigilance face aux e-mails suspects ;
- protection des identifiants ;
- verrouillage des postes de travail ;
- respect des règles internes de confidentialité.

12. Contrôle et amélioration

La politique de sécurité est réévaluée :

- en cas d'incident ;
- lors de changements techniques ;
- au minimum une fois tous les trois ans.

Des améliorations peuvent être mises en œuvre pour renforcer la sécurité des données.

CHAPITRE 6 – Gestion des violations de données personnelles

1. Objet

La présente procédure décrit les actions à mettre en œuvre en cas de violation de données personnelles au sein de la Scierie Ehrstein.

Une violation de données peut avoir des conséquences graves sur les droits et libertés des personnes concernées. Cette procédure vise à limiter les impacts et à respecter les obligations légales de notification.

2. Définition d'une violation de données

Une violation de données personnelles est toute situation entraînant :

- la perte de données ;
- la destruction accidentelle ou illégale de données ;
- l'altération de données ;
- la divulgation non autorisée de données ;
- l'accès non autorisé à des données personnelles.

Exemples :

- vol ou perte d'un ordinateur contenant des fichiers clients ;
- piratage d'un compte Microsoft 365 ;
- envoi d'un e-mail à un mauvais destinataire ;
- ransomware bloquant l'accès au NAS ;
- suppression accidentelle de fichiers clients.

3. Objectifs de la procédure

- Réagir rapidement en cas d'incident ;
- Limiter les impacts sur les personnes concernées ;
- Protéger les systèmes d'information ;
- Respecter les obligations de notification à la CNIL ;
- Documenter les incidents.

4. Détection et signalement

Toute personne constatant un incident doit immédiatement :

- informer un des gérants ;
- décrire précisément l'incident ;
- indiquer les données potentiellement concernées ;
- préciser la date et les circonstances.

5. Mesures immédiates

Dès la détection d'une violation, la Scierie Ehrstein met en œuvre les actions suivantes :

1. **Isoler l'incident** (déconnexion du poste ou du système concerné si nécessaire) ;
2. **Limitier l'accès aux données concernées** ;
3. **Sécuriser les comptes utilisateurs** (changement de mots de passe, blocage des accès) ;
4. **Évaluer l'étendue de la violation** ;
5. **Lancer la restauration des données via les sauvegardes si nécessaire.**

6. Analyse de la violation

La direction procède à une analyse :

- nature des données concernées ;
- nombre de personnes impactées ;
- gravité du risque pour les personnes ;
- origine de l'incident ;
- mesures correctives à mettre en place.

7. Notification à la CNIL

Conformément au RGPD, la violation doit être notifiée à la CNIL dans un délai de **72 heures** si elle est susceptible d'engendrer un risque pour les droits et libertés des personnes.

La notification contient notamment :

- la nature de la violation ;

- les catégories et le nombre approximatif de personnes concernées ;
- les conséquences probables ;
- les mesures prises ou proposées pour remédier à la violation.

8. Information des personnes concernées

Lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, celles-ci sont informées dans les meilleurs délais.

L'information précise :

- la nature de la violation ;
- les conséquences possibles ;
- les mesures prises ;
- les recommandations pour se protéger.

9. Mesures correctives

À la suite d'une violation, la Scierie Ehrstein met en place :

- correction des failles de sécurité identifiées ;
- renforcement des mots de passe et accès ;
- amélioration des procédures internes ;
- formation ou sensibilisation complémentaire ;
- vérification des sauvegardes.

10. Documentation des incidents

Chaque violation de données est consignée dans un registre interne comprenant :

- date de l'incident ;
- description ;
- données concernées ;
- nombre de personnes impactées ;
- mesures prises ;
- notification CNIL (oui/non) ;
- actions correctives.

11. Responsable de la gestion des incidents

La gestion des violations est assurée par les gérants de la Scierie Ehrstein :

- Laurent Ehrstein
- Jacky Ehrstein
- Elise Ehrstein

Ils sont responsables de l'évaluation, de la notification et de la mise en œuvre des mesures correctives.

12. Amélioration continue

Chaque incident donne lieu à une analyse afin de prévenir sa réapparition.

La présente procédure est mise à jour régulièrement en fonction des évolutions techniques et réglementaires.

CHAPITRE 7 – Procédure d'exercice des droits des personnes

1. Objet

La présente procédure définit les modalités permettant aux personnes concernées d'exercer leurs droits prévus par le Règlement (UE) 2016/679 (RGPD), ainsi que les modalités de traitement de ces demandes par la Scierie Ehrstein.

2. Droits des personnes concernées

Toute personne dont les données sont traitées par la Scierie Ehrstein dispose des droits suivants :

- droit d'accès ;
- droit de rectification ;
- droit à l'effacement (dans les limites légales) ;
- droit à la limitation du traitement ;
- droit d'opposition ;
- droit à la portabilité des données (lorsque applicable).

3. Modalités de demande

Les demandes peuvent être adressées :

- par e-mail : info@scierie-ehrstein.com
- par courrier postal :
Scierie Ehrstein
2, rue de la Sauer
67510 Lembach – France

La demande doit préciser :

- l'identité du demandeur ;
- le droit exercé ;
- toute information permettant d'identifier les données concernées.

4. Vérification de l'identité

Avant de répondre à une demande, la Scierie Ehrstein peut demander des informations complémentaires afin de vérifier l'identité du demandeur lorsque cela est nécessaire.

Cette vérification vise à éviter toute divulgation non autorisée de données personnelles.

5. Délais de réponse

La Scierie Ehrstein s'engage à répondre à toute demande dans un délai maximum de :

- **1 mois** à compter de la réception de la demande.

Ce délai peut être prolongé de 2 mois supplémentaires en cas de demande complexe ou de volume important de requêtes.

Le demandeur est alors informé de cette prolongation.

6. Traitement des demandes

Une fois la demande reçue :

1. La demande est enregistrée dans le registre interne ;
2. Les données concernées sont identifiées ;
3. Une analyse de conformité est réalisée ;
4. Une réponse est préparée ;
5. La réponse est envoyée au demandeur.

7. Réponse aux demandes

7.1 Droit d'accès

La personne peut obtenir une copie des données la concernant ainsi que des informations sur leur traitement.

7.2 Droit de rectification

Les données inexactes ou incomplètes peuvent être corrigées.

7.3 Droit à l'effacement

Les données peuvent être supprimées lorsque :

- elles ne sont plus nécessaires ;
- la personne retire son consentement (si applicable) ;
- le traitement est illicite.

Certaines données ne peuvent pas être supprimées lorsqu'elles sont nécessaires à des obligations légales (ex : facturation).

7.4 Droit d'opposition

La personne peut s'opposer à certains traitements fondés sur l'intérêt légitime.

7.5 Droit à la limitation

Le traitement peut être temporairement suspendu dans certains cas.

8. Conservation des demandes

Toutes les demandes relatives aux droits RGPD sont enregistrées dans un registre interne comprenant :

- date de la demande ;
- identité du demandeur ;
- type de droit exercé ;
- réponse apportée ;
- date de clôture.

Ces informations sont conservées pendant **3 ans** à des fins de traçabilité.

9. Refus de demande

Une demande peut être refusée lorsque :

- elle est manifestement infondée ou excessive ;
- la loi impose la conservation des données ;
- l'identité du demandeur ne peut pas être vérifiée.

Le refus est motivé et expliqué au demandeur.

10. Communication des données

Les données sont transmises :

- de manière sécurisée ;
- dans un format lisible ;
- sans porter atteinte aux droits de tiers.

11. Responsable du traitement des demandes

Les demandes sont traitées par les gérants de la Scierie Ehrstein :

- Laurent Ehrstein
- Jacky Ehrstein
- Elise Ehrstein

12. Amélioration continue

La procédure est révisée régulièrement afin d'assurer :

- la conformité réglementaire ;
- la rapidité de traitement des demandes ;
- la sécurité des données transmises.

CHAPITRE 8 – Registres internes RGPD

1. Objet

Ce chapitre présente les modèles de registres internes utilisés par la Scierie Ehrstein pour assurer la traçabilité de sa conformité au Règlement Général sur la Protection des Données (RGPD).

Ces registres permettent de démontrer la bonne gestion des demandes des personnes concernées et des éventuelles violations de données.

2. Registre des demandes d'exercice des droits

2.1 Finalité

Ce registre permet de documenter toutes les demandes reçues au titre des droits RGPD (accès, rectification, suppression, opposition, limitation, portabilité).

2.2 Contenu du registre

Chaque demande est enregistrée avec les informations suivantes :

- Date de réception de la demande
- Identité du demandeur
- Type de droit exercé
- Description de la demande
- Vérification de l'identité (oui/non)
- Réponse apportée
- Date de réponse
- Action réalisée (accès, suppression, modification, refus motivé)
- Observations éventuelles

2.3 Exemple de registre

Date	Demandeur	Droit exercé	Action	Date réponse	Statut
15/03/2026	Client X	Accès	Extraction des données	20/03/2026	Clôturée
02/04/2026	Prospect Y	Suppression	Données supprimées	05/04/2026	Clôturée

2.4 Conservation

Les informations du registre sont conservées pendant **3 ans** à compter de la clôture de la demande.

3. Registre des violations de données

3.1 Finalité

Ce registre recense l'ensemble des incidents de sécurité ayant un impact sur les données personnelles.

Il permet de démontrer la capacité de l'entreprise à détecter, analyser et corriger les incidents.

3.2 Contenu du registre

Chaque incident est documenté avec :

- Date de l'incident
- Date de détection
- Nature de la violation
- Catégorie de données concernées
- Nombre de personnes impactées
- Cause de l'incident
- Mesures prises immédiatement
- Notification à la CNIL (oui/non)
- Information des personnes concernées (oui/non)
- Actions correctives mises en place
- Responsable du traitement de l'incident

3.3 Exemple de registre

Date	Incident	Données concernées	Impact	CNIL	Actions
10/06/2026	Envoi e-mail erroné	Coordonnées client	1 personne	Non	Récupération + suppression
22/06/2026	Compte compromis	Emails	Limité	Oui	Reset + MFA activé

3.4 Conservation

Le registre des violations est conservé pendant **5 ans**.

4. Responsable des registres

La tenue et la mise à jour des registres sont assurées par les gérants de la Scierie Ehrstein :

- Laurent Ehrstein
- Jacky Ehrstein
- Elise Ehrstein

5. Mise à jour

Les registres doivent être mis à jour :

- immédiatement après chaque demande ou incident ;
- lors des audits internes ;
- lors des évolutions des systèmes ou procédures.

6. Importance des registres

Ces documents constituent une preuve essentielle de conformité au RGPD.

Ils doivent pouvoir être présentés à tout moment en cas de contrôle de la CNIL.

CHAPITRE 9 – Charte de confidentialité des salariés et collaborateurs

1. Objet

La présente charte définit les règles de confidentialité et de protection des données personnelles applicables à l'ensemble des salariés, collaborateurs et personnes habilitées à traiter des données au sein de la Scierie Ehrstein.

Elle s'inscrit dans le cadre du Règlement (UE) 2016/679 (RGPD) et des obligations légales en vigueur.

2. Champ d'application

La présente charte s'applique à toute personne ayant accès, même occasionnellement, à des données personnelles dans le cadre de ses fonctions :

- salariés ;

- gérants ;
- apprentis ;
- prestataires intervenant sur les systèmes d'information.

3. Principe de confidentialité

Toute personne ayant accès à des données personnelles s'engage à :

- ne pas divulguer les données à des tiers non autorisés ;
- ne pas utiliser les données à des fins personnelles ;
- respecter la finalité des traitements ;
- garantir la confidentialité des informations traitées.

Cette obligation reste valable même après la fin de la relation de travail.

4. Accès aux données

L'accès aux données est strictement limité :

- aux seules personnes dont les missions le justifient ;
- aux outils nécessaires à l'activité professionnelle ;
- aux droits d'accès définis par la direction.

Toute tentative d'accès non autorisé est interdite.

5. Utilisation des outils informatiques

Les utilisateurs s'engagent à :

- utiliser les outils professionnels uniquement à des fins professionnelles ;
- respecter les consignes de sécurité ;
- ne pas installer de logiciels non autorisés ;
- verrouiller leur poste de travail en cas d'absence ;
- signaler toute anomalie ou incident de sécurité.

6. Gestion des mots de passe

Les mots de passe sont strictement personnels et ne doivent jamais être communiqués à un tiers.

Il est interdit :

- de partager ses identifiants ;
- d'écrire ses mots de passe de manière non sécurisée ;
- de réutiliser un mot de passe sur plusieurs services.

7. Utilisation des données clients et fournisseurs

Les données ne peuvent être utilisées que dans le cadre :

- de la relation commerciale ;
- des obligations administratives ;
- des tâches confiées par la direction.

Toute utilisation à des fins personnelles est strictement interdite.

8. Sécurité et vigilance

Les utilisateurs doivent faire preuve de vigilance notamment face :

- aux e-mails suspects (phishing) ;
- aux pièces jointes inconnues ;
- aux demandes inhabituelles de données ;
- aux tentatives d'usurpation d'identité.

Tout incident doit être immédiatement signalé à la direction.

9. Télétravail et accès à distance

En cas d'accès à distance :

- les connexions doivent être sécurisées ;
- les équipements doivent être protégés ;
- les environnements de travail doivent rester confidentiels.

10. Sanctions

Tout manquement à la présente charte peut entraîner :

- un rappel à l'ordre ;
- des mesures disciplinaires ;
- des sanctions prévues par le droit du travail ;
- des poursuites en cas de violation grave.

11. Entrée en vigueur

La présente charte est applicable dès sa communication à l'ensemble des personnes concernées.

12. Engagement

Chaque personne habilitée à traiter des données personnelles au sein de la Scierie Ehrstein reconnaît avoir pris connaissance de la présente charte et s'engage à la respecter.

CHAPITRE 10 – Engagement de confidentialité

1. Objet

Le présent engagement formalise l'obligation de confidentialité des personnes ayant accès aux données personnelles traitées par la Scierie Ehrstein.

Il complète la charte de confidentialité interne et s'applique à toute personne autorisée à accéder aux systèmes ou aux données de l'entreprise.

2. Engagement de confidentialité

Je soussigné(e),

Nom : _____

Prénom : _____

Fonction : _____

Reconnais avoir accès, dans le cadre de mes fonctions au sein de la Scierie Ehrstein, à des informations et données à caractère personnel.

Je m'engage à :

- respecter la confidentialité des données auxquelles j'ai accès ;
- ne pas divulguer ces données à des personnes non autorisées ;
- utiliser les données uniquement dans le cadre de mes fonctions professionnelles ;
- respecter les consignes de sécurité mises en place par l'entreprise ;
- signaler immédiatement tout incident ou suspicion de violation de données.

3. Protection des données

Je reconnais que les données traitées peuvent concerner notamment :

- des clients ;
- des prospects ;
- des fournisseurs ;
- des partenaires commerciaux ;
- des informations internes de l'entreprise.

Je m'engage à ne pas les utiliser à des fins personnelles ou étrangères à mes missions.

4. Durée de l'engagement

Le présent engagement est valable pendant toute la durée de la relation contractuelle avec la Scierie Ehrstein.

Il demeure applicable après la fin de la relation de travail ou de collaboration, sans limitation de durée, pour toutes les informations dont j'aurai eu connaissance.

5. Sanctions

Tout manquement au présent engagement peut entraîner :

- des sanctions disciplinaires ;
- la résiliation du contrat de travail ou de prestation ;
- des poursuites civiles et/ou pénales conformément à la législation en vigueur.

6. Signature

Fait à : _____

Le : _____

Signature précédée de la mention « Lu et approuvé » :

7. Conservation

Le présent engagement est conservé par la Scierie Ehrstein pendant toute la durée de la relation contractuelle, puis archivé conformément aux obligations légales applicables.

CHAPITRE 11 – Synthèse du dispositif RGPD

1. Objectif de la synthèse

Ce chapitre présente une vision globale des mesures mises en place par la Scierie Ehrstein afin d'assurer sa conformité au Règlement Général sur la Protection des Données (RGPD).

2. Gouvernance des données

La responsabilité du traitement des données personnelles est assurée par les gérants de l'entreprise :

- Laurent Ehrstein
- Jacky Ehrstein
- Elise Ehrstein

Ils veillent à la mise en œuvre et au respect des règles internes de protection des données.

3. Nature des données traitées

La Scierie Ehrstein traite uniquement des données nécessaires à son activité :

- données d'identification (nom, prénom) ;
- coordonnées (adresse, téléphone, e-mail) ;
- données de facturation ;
- données liées aux devis et commandes.

Aucune donnée sensible n'est traitée.

4. Finalités des traitements

Les données sont utilisées exclusivement pour :

- la gestion des demandes de contact ;
- l'établissement de devis ;
- la gestion des commandes ;
- la facturation ;
- le suivi client ;
- le respect des obligations légales.

5. Mesures techniques et organisationnelles

Les principales mesures mises en œuvre sont :

- hébergement du site chez OVH ;
- utilisation de Microsoft 365 pour la messagerie et les documents ;
- utilisation du logiciel de facturation ANT ;
- stockage local sur NAS sécurisé ;
- sauvegardes hebdomadaires ;
- gestion des accès par identifiants personnels ;
- politique de mots de passe renforcée ;
- sensibilisation du personnel.

6. Conservation des données

Les données sont conservées selon des durées strictement définies :

- 3 ans pour les prospects ;
- durée de la relation commerciale pour les clients ;
- 10 ans pour les obligations comptables ;
- suppression ou archivage sécurisé à expiration.

7. Droits des personnes

Les personnes concernées disposent des droits suivants :

- accès ;
- rectification ;
- suppression ;
- opposition ;
- limitation ;
- portabilité.

Les demandes sont traitées sous 1 mois.

8. Gestion des incidents

Une procédure de gestion des violations de données est en place afin de :

- limiter les impacts ;
- sécuriser les systèmes ;
- notifier la CNIL si nécessaire ;
- informer les personnes concernées en cas de risque élevé.

9. Documentation et traçabilité

La conformité est documentée à travers :

- registre des traitements ;
- registre des demandes RGPD ;
- registre des violations ;
- politique de sécurité ;
- politique de conservation ;
- chartes internes.

10. Amélioration continue

Le dispositif RGPD est régulièrement mis à jour afin de :

- suivre les évolutions réglementaires ;
- adapter les outils utilisés ;
- améliorer la sécurité des systèmes ;
- renforcer les bonnes pratiques internes.

11. Conclusion

La Scierie Ehrstein met en œuvre un ensemble de mesures organisationnelles et techniques proportionnées à son activité afin de garantir la protection des données personnelles et le respect du RGPD.

ANNEXES RGPD

Annexe 1 – Mention RGPD formulaire de contact

« Les informations recueillies via ce formulaire sont enregistrées par la Scierie Ehrstein afin de répondre à votre demande de contact ou de devis. Elles sont conservées pendant 3 ans et ne sont pas transmises à des tiers. Vous disposez d'un droit d'accès, de rectification et de suppression en nous contactant à : info@scierie-ehrstein.com »

Annexe 2 – Case à cocher formulaire

☐ J'accepte que mes données soient utilisées pour traiter ma demande conformément à la politique de confidentialité.

Annexe 3 – Texte bandeau cookies

« Ce site utilise uniquement des cookies nécessaires à son fonctionnement. Aucun cookie de suivi publicitaire n'est utilisé sans votre consentement. »

Annexe 4 – Modèle réponse demande RGPD

Objet : Votre demande relative à vos données personnelles

Bonjour,

Nous accusons réception de votre demande concernant l'exercice de vos droits au titre du RGPD.

Votre demande est actuellement en cours de traitement. Une réponse vous sera apportée dans un délai maximum d'un mois.

Cordialement,
Scierie Ehrstein

Annexe 5 – Modèle suppression de données

Objet : Traitement de votre demande de suppression

Bonjour,

Nous vous informons que vos données personnelles ont été supprimées de nos systèmes, à l'exception de celles que nous sommes légalement tenus de conserver.

Cordialement,
Scierie Ehrstein

Annexe 6 – Checklist interne RGPD

- ☐ Mise à jour du registre des traitements
- ☐ Vérification des sauvegardes hebdomadaires
- ☐ Contrôle des accès utilisateurs
- ☐ Suppression des données obsolètes
- ☐ Mise à jour des mots de passe
- ☐ Vérification des sous-traitants (OVH, Microsoft 365, ANT)