

ROBERT RENAUD SA

POLITIQUE DE
CONFIDENTIALITÉ DES
DONNÉES

Contenu

I.	Préambule/ Objectif	3
II.	Définitions	3
III.	Champ d'application.....	4
IV.	Principes	5
1.	Traitements	5
2.	Sécurité Informatique	6
3.	Lignes directrices	7
V.	Transferts des données	8
VI.	Violation et fuite de données	8
VII.	Droits des personnes concernées	8
VIII.	Directives détaillées	9
1.	Politique de transparence	9
2.	Délais	10
3.	Droit d'accès, droit de rectification et droit à l'oubli	10
4.	Portabilité des données	11
IX.	Contrôle des données.....	11
X.	Date d'entrée en vigueur	11

Politique de confidentialité interne et déclaration de protection des données de la société Renaud

I. Préambule/ Objective

Robert Renaud SA une entreprise privée suisse spécialisée dans la conception et la fabrication de broches. Membre de Smart Industries SA et du groupe Rollomatic, Robert Renaud SA partage des valeurs fondamentales telles que la passion pour la technologie de haute précision, le savoir-faire suisse, la recherche constante de la qualité et l'esprit d'entreprise. Un comportement irréprochable contribue directement à la réalisation de ses objectifs, de même que le respect de la confidentialité des données.

Robert Renaud SA s'engage à respecter la confidentialité des données dans l'ensemble de la société et dans le cadre de la collaboration avec ses partenaires commerciaux.

Dans le cadre de ses activités quotidiennes, Robert Renaud SA traite donc une variété de données personnelles. À cet égard et dans le cadre de la présente politique, Robert Renaud SA poursuit les objectifs suivants :

- Mise en place d'une norme minimale uniforme à appliquer en matière de traitement des données personnelles.
- Fournir des garanties préventives contre la violation des droits de la personnalité et de la vie privée par le biais d'un traitement inapproprié des données personnelles.
- Assurer un niveau de protection adéquat des données personnelles comme l'exige le règlement (notamment la loi suisse sur la protection des données et le règlement général sur la protection des données de l'Union européenne).
- Fournir une information transparente sur les données personnelles traitées par Renaud, la manière et l'objectif du traitement de ces données par Renaud et les droits des personnes concernées par le traitement des données par Renaud.

En outre, la protection des données et les autres lois locales applicables qui prévoient des règles obligatoires plus strictes doivent également être respectées. Les collaborateurs qui ont des doutes quant à l'obligation de respecter ces lois locales en plus des règles énoncées dans la présente politique doivent contacter le service des ressources humaines.

II. Définitions

"Traitement actif" désigne toute opération qui va au-delà de la réception sans demande et de la conservation d'une trace générée automatiquement dans un système informatique.

"Données de base" ont la signification décrite à la section VIII ci-dessous.

"Données" désigne toute information relative à une personne physique identifiée ou identifiable.

"Personne concernée" désigne toute personne physique dont les données personnelles sont traitées par ou pour le compte de Robert Renaud SA.

"LPD" désigne la loi suisse sur la protection des données, telle que modifiée de temps à autre.

"EEE" désigne la liste des Pays mentionnés dans l'annexe 1 de l'Ordonnance sur la protection des données, qui peut être modifiée de temps à autre.

"Salariés" désigne une personne travaillant pour Robert Renaud SA en tant qu'employé ou occupant un poste similaire tel qu'un sous-traitant.

"RGPD" désigne le Règlement général sur la protection des données, qui peut être modifiée de temps à autre.

" Données relatives aux RH " a le sens qui lui est donné à la section VIII ci-dessous.

" Données diverses " a le sens qui lui est donné à la section VIII ci-dessous.

" Données passives" a le sens qui lui est donnée à la section VIII ci-dessous.

"Données personnelles" désigne toute information qui se rapporte à une personne physique identifiée ou identifiable ; Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, ou à un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique. Il peut s'agir d'un nom, d'une adresse e-mail, d'une adresse IP, d'une date de naissance, d'une sécurité sociale, photos, etc.

"Politique" désigne la présente politique de confidentialité et déclaration de protection des données de Robert Renaud SA.

"Traitement" ou "Traitée" désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou à des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison, la restriction, la suppression ou la destruction.

"Réglementation" désigne la loi suisse sur la protection des données (LPD) et le règlement général sur la protection des données (RGPD), tels que modifiés de temps à autre.

III. Champs d'application

La présente politique s'applique également aux éventuels sous-traitants de données qui traitent et stockent des données pour le compte de Robert Renaud SA.

IV. Principes

1. Traitement

Robert Renaud SA a pour objectif d'assurer le respect du Règlement. Le Règlement repose sur huit principes importants, stipulant que les données à caractère personnel doivent être :

- traitées de manière loyale et licite ;
- obtenus uniquement à des fins licites spécifiques ;
- adéquates, pertinentes et non excessives ;
- exactes et tenues à jour ;
- conservées pendant une durée n'excédant pas celle nécessaire ;
- traitées conformément aux droits des personnes concernées ;
- protégées par des moyens technique et organisationnelle appropriée ;
- En cas de transmission en dehors de l'EEE, des mesures appropriées doivent être mises en place.

Les employés doivent traiter les données à caractère personnelles conformément à ces principes. En particulier, les employés ne traiteront pas de données à caractère personnel, sauf si l'une des conditions suivantes est remplie :

- la personne concernée a consenti à ce traitement (si le consentement est requis pour un tel traitement) ;
- Renaud doit effectuer ce traitement (i) pour exécuter ou prendre des mesures en vue de conclure un contrat avec la personne concernée, (ii) pour se conformer à une obligation légale de Renaud ou (iii) pour protéger les intérêts vitaux de la personne concernée dans une situation de "vie ou de mort" ; ou
- Robert Renaud SA a besoin d'effectuer cette procédure pour poursuivre ses intérêts légitimes. Ces intérêts ne sont pas négligés du fait que le traitement porte atteinte aux intérêts ou aux libertés et droits fondamentaux de la personne concernée.

Robert Renaud SA ne traite pas activement les données personnelles. En d'autres termes, elle n'exerce aucune activité commerciale avec une telle collecte de données. Les données personnelles ne sont collectées que pour soutenir l'activité commerciale sur la base du besoin.

Les données personnelles traitées par Robert Renaud SA sont réparties dans les quatre catégories suivantes. Ces catégories sont prévues pour faciliter la mise en œuvre des lignes directrices fournies par le règlement :

- **Données relatives aux employés et autres données stockées dans un système tel qu'un logiciel (ci-après « Données de base »)**

Les données à caractère personnel relatives aux dossiers des employés, au traitement de la paie et des assurances sociales et à la comptabilité (y compris le système ERP) sont traitées pour des raisons liées au département des ressources humaines. Conformément au Règlement, le traitement des données à caractère personnel des employés n'est pas basé sur un consentement mais sur un intérêt légitime.

- **Données d'autres personnes collectées dans le cadre des procédures de ressources humaines (ci-après « Données relatives aux RH »)**

Données personnelles des candidats collectées à des fins de recrutement.

- **Données d'autres personnes collectées dans le cadre d'activités commerciales (ci-après « Données diverses »)**

Données à caractère personnel relatives aux salariés d'une entité légale (clients) collectées dans le cadre d'échanges commerciaux. Ces données sont collectées pour permettre la communication entre Robert Renaud SA et ses clients et pour mieux comprendre les besoins des clients en lien avec les produits et services Robert Renaud SA.

- **Données collectées passivement (ci-après « Données passives »)**

Données personnelles collectées par e-mail ou appels téléphoniques par la société et stockées sans aucun traitement actif (adresses e-mail, numéro de téléphone, etc.).

2. Sécurité informatique

Les mesures techniques, organisationnelles et juridiques nécessaires pour préserver la sécurité et la confidentialité des données à caractère personnel sont prises en fonction des risques posés liés aux traitements effectués des données concernées à caractère sensible ou non. Nous nous efforçons en permanence d'améliorer ces mesures pour préserver la sécurité des données à caractère personnel.

La politique informatique de Robert Renaud SA permet aux employés de travailler dans un bon environnement, équipé d'une technologie de pointe. L'accent est mis sur la sécurité périmétrique et la protection des données, en contrôlant scrupuleusement les accès (internes et externes), en limitant les installations de programmes non autorisées et en assurant la résilience et la sauvegarde de tous nos systèmes, pour ne citer que quelques exemples de cette politique informatique. De plus, plusieurs mesures sont prises pour assurer une défense optimale contre les attaques de cybersécurité. Des formations et des avertissements sont fournis aux employés.

Les mesures techniques, organisationnelles et juridiques nécessaires pour préserver la sécurité et la confidentialité des données à caractère personnel sont prises en fonction des

risques posés liés aux traitements effectués des données concernées à caractère sensible ou non. Nous nous efforçons en permanence d'améliorer ces mesures pour préserver la sécurité des données à caractère personnel.

3. Lignes directrices

Afin de respecter les principes de protection des données lors du traitement des données personnelles, les employés doivent respecter les directives générales suivantes :

- Les seuls à pouvoir accéder aux données personnelles sont les personnes qui en ont besoin dans le cadre de leur travail ;
- les employés doivent collecter le moins de données personnelles possible, c'est-à-dire uniquement les données personnelles nécessaires à l'activité de Robert Renaud SA et dans le respect du règlement et des autres lois applicables ;
- les employés reconnaissent les données personnelles contenant des informations sensibles, telles que la race, la religion, la santé, les données biométriques, etc. Ces données nécessitent une protection juridique supplémentaire. Le traitement de ce type de données personnelles n'est pas autorisé. Veuillez contacter le service des ressources humaines pour obtenir une approbation préalable ;
- les données personnelles ne peuvent être traitées que sur la base d'un motif légal. Veuillez contacter le service des ressources humaines pour obtenir des informations sur ces motifs ;
- les données personnelles doivent être régulièrement examinées et mises à jour si elles sont jugées obsolètes. Si elles ne sont plus nécessaires, elles doivent être supprimées et éliminées ;
- si des données personnelles doivent être transmises à des pays en dehors de l'EEE ou si un accès à distance est accordé depuis des pays en dehors de l'EEE à des données personnelles au sein de l'EEE, les employés doivent d'abord contacter le service des ressources humaines avant d'effectuer de telles transmissions ;
- les données personnelles ne doivent jamais être partagées de manière informelle. Lorsque l'accès à des informations confidentielles est requis, les employés doivent en faire la demande auprès du service des ressources humaines ;
- Les données personnelles ne doivent jamais être divulguées à des personnes non autorisées. En particulier, des mots de passe robustes doivent être utilisés et ne jamais être partagés ;
- lors de l'échange d'informations par courrier électronique ou par des méthodes similaires, les employés doivent veiller à ce qu'aucune donnée personnelle ne soit communiquée inutilement (par exemple, en utilisant Cci au lieu de Cc afin d'éviter de partager les adresses électroniques avec d'autres destinataires) ;

- Les données à caractère personnel conservées sous format papier doivent être enfermées dans un tiroir ou un classeur, et ne doivent pas être laissées dans un endroit où des personnes non autorisées pourraient les voir, par exemple sur une imprimante. Les documents imprimés contenant des données à caractère personnel doivent être déchiquetés et éliminés de manière sûre lorsqu'ils ne sont plus nécessaires ;
- Les employés doivent garder leur bureau bien rangé. Un bureau bien rangé réduit la possibilité d'une fuite de données ;
- Les données personnelles stockées électroniquement sont soumises à des directives spécifiques, décrites ci-dessous dans la section VIII ;
- Les employés doivent demander l'aide du département des ressources humaines en cas de doute sur le traitement des données personnelles.

V. Transferts transfrontaliers de données

En règle générale, toutes les données personnelles sont traitées en Suisse. Dans l'hypothèse où des données personnelles seraient transmises à l'étranger et en particulier vers des pays tiers en dehors de l'EEE, Robert Renaud SA mettra en œuvre les clauses contractuelles types de l'UE.

VI. Violation et fuite de données

Toute violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès à des données personnelles transmises, stockées ou traitées d'une autre manière constitue une violation ou une fuite potentielle de données (par exemple, piratage informatique, fichiers numériques volés ou listes imprimées contenant des données personnelles ou perte d'une clé USB ou d'un autre dispositif contenant des données personnelles).

Si une telle violation ou fuite de données personnelles se produit, Renaud est légalement tenu de la signaler à l'autorité chargée de la protection des données dans les 72 heures.

Les employés qui ont connaissance d'une violation ou d'une fuite de données sont tenus de contacter immédiatement un membre de la direction ou du département des ressources humaines.

VII. Droits des personnes concernées

Les personnes concernées par le traitement de données à caractère personnel doivent en être informées sur demande. Elles ont notamment le droit d'être informées des finalités pour lesquelles les données à caractère personnel sont traitées, de la catégorie de données concernée et de l'identité des destinataires des données.

Le cas échéant, les personnes concernées ont également le droit d'exiger que les données à caractère personnel soient rectifiées, bloquées ou effacées (y compris le droit à l'oubli), que le

traitement soit limité ou de s'opposer à un tel traitement, ainsi que le droit à la portabilité des données (obtenir une copie des données à caractère personnel pour les réutiliser avec un autre service ou une autre organisation). Si les employés reçoivent de telles demandes, ils doivent immédiatement contacter le département des ressources humaines. Pour plus de détails, veuillez-vous référer à la section VIII ci-dessous.

VIII. Directives détaillées

Les lignes directrices suivantes permettent d'assurer le respect des principes édictés par le Règlement.

1 Principe de transparence

Selon le règlement, l'information et la communication relatives au traitement des données doivent être facilement accessibles, faciles à comprendre et formulées en termes clairs et simples. En particulier, la personne doit être informée des risques, des règles, des garanties et des droits liés au traitement des données. Le règlement offre également à la personne concernée la garantie d'être informée des modalités d'exercice de ses droits (identité du responsable du traitement, finalité du traitement, droit d'obtenir la confirmation et la communication des données à caractère personnel concernées, etc.)

Ce principe s'applique comme suit :

- **Données de base** collectées dans le cadre d'un processus de recrutement aboutissant à un engagement, le contrat de travail fournit des informations adéquates conformément à la Politique ;
-
- **Données relatives aux ressources humaines** collectées dans le cadre d'un recrutement infructueux : ces données sont conservées pendant une durée de cinq (5) ans puis automatiquement détruites. Les candidats peuvent trouver des informations détaillées sur cette politique sur le site Web de la société. Si le candidat à l'emploi peut s'opposer à une conservation de ses données personnelles pendant une durée de 5 ans, ses données sont supprimées sans délai. En outre, il est précisé que les données du candidat ne sont collectées qu'en relation avec le poste et limitées aux informations utiles pour déterminer le niveau de compétence du candidat.
- **Les Données Diverses** comprennent les données collectées lors de l'inscription d'un utilisateur à la « Newsletter » de la Société, pour une demande d'accès Wi-Fi de la société (en cas de visite), pour un accès aux outils numériques et portails de la Société tels que (mais non exclusivement) « MyRenaud ». Ces données diverses sont conservées uniquement pour permettre une prise de contact avec la personne concernée. Pour plus d'informations sur les données diverses, les personnes concernées peuvent consulter la Politique ainsi que la politique de gestion des données sur le site internet de la Société ;
- **Les Données passives**, Les données passives n'étant pas traitées activement, aucune autre mesure n'est prévue, à l'exception du principe général de sécurité.

2. Délais

Selon le Règlement, une durée de conservation des Données doit être définie et limitée au strict minimum.

Ce principe s'applique de la manière suivante :

- La conservation des données de base est requise par un certain nombre de dispositions légales et est également utile dans l'intérêt des employés (par exemple, les données personnelles requises pour les assurances sociales après le départ de l'employé de l'entreprise). Ces données sont conservées sans limite de temps (ce que l'on appelle « l'intérêt légitime ») ;
- Les Données relatives aux RH : Lorsque l'engagement a pris fin, seules peuvent être conservées les données indispensables telles que les données à conserver en vertu d'une obligation légale (par ex. comptables, sociales ou fiscales) ou celles dont la conservation est dans l'intérêt de l'employé (documents nécessaires à l'établissement d'un certificat, par exemple). Peuvent également être conservées les données dont l'employeur a besoin pour un litige pendant. La durée de conservation est définie au cas par cas, en fonction de la catégorie de données. Elle sera généralement fixée à 5 - 10 ans en fonction de ce que la loi le prescrit. Dans les autres cas, les données doivent être détruites dès que leur conservation n'est plus requise. L'employé conserve son droit d'accès fixé à l'art. 25 LPD même lorsque ses rapports de travail ont pris fin.
- Étant donné que l'entreprise n'est pas en mesure de déterminer si les données diverses sont encore utiles ou pertinentes (si la personne travaille-t-elle encore pour le client ou non), ce type de données n'est supprimé que sur demande ;
- **Les données passives** n'étant pas traitées activement, aucune autre mesure que le principe général de sécurité n'est prévue.

3. Droit d'accès, droit de rectification et droit à l'oubli

Le règlement prévoit que des mesures appropriées doivent être prises pour que les données à caractère personnel inexacts soient rectifiées ou effacées. Des modalités doivent être prévues pour faciliter l'exercice des droits conférés.

Ce principe s'applique de la manière suivante :

- Chaque employé a le droit de demander gratuitement l'accès à ses données de base et le droit de demander une rectification de ses données. Pour les raisons mentionnées ci-dessus, un employé ne peut pas demander la suppression de ses données personnelles ;
- Chaque candidat non retenu a le droit d'accéder à ses données enregistrées auprès des ressources humaines et d'en demander la rectification et la suppression, sans frais ;

- Chaque personne, dont les données sont conservées, a le droit de demander gratuitement l'accès à ses **données diverses** et de demander leur rectification, ainsi que leur suppression ;
- **Les données passives** n'étant pas traitées activement, aucune autre mesure que le principe général de sécurité n'est prévue.

4. Transfers des données

Conformément au Règlement, la personne concernée a le droit de transférer gratuitement ses données personnelles dans un format standard.

Ce principe s'applique de la manière suivante :

- La Société accorde ce droit à toutes les personnes concernées, pour les **données de base**, les **données liées aux RH** et les **données diverses** ;
- Les données passives n'étant pas traitées activement, aucune autre mesure que le principe général de sécurité n'est prévue.

IX. Contrôle des données

La personne responsable du département RH de Robert Renaud SA est responsable du traitement des données. Elle détermine seule ou conjointement avec d'autres, les finalités et les moyens du traitement conformément au Règlement. Pour toute demande, relative aux droits prévus par le Règlement, le service RH peut être contacté à l'adresse électronique suivante : rh@renaud.ch.

Un registre des activités de traitement des données est tenu.

En Suisse, la possibilité est accordée de déposer une réclamation auprès de l'autorité de contrôle désignée en cas de non-respect des droits en matière de protection des données. L'autorité de contrôle compétente est le préposé fédéral à la protection des données et à la transparence.

X. Date d'entrée en vigueur

La présente politique est entrée en vigueur le 1er septembre 2023.