

## Traduction libre

### Contrat de protection de données pour la sous-traitance en application de l'article 28 du RGPD

Au nom de :

Traité par :

Softgarden e-recruiting GmbH  
Tauentzienstrasse 14  
10789 Berlin, Germany

Ci-après dénommé "**Client**"

Ci-après dénommé « **Sous-traitant** »

Ci-après dénommés ensemble « **partenaires contractuels** ».

#### §1 Généralités

1. Le Sous-traitant traite les données personnelles pour le compte du Client au sens de l'article 4 n°8 et article 28 du Règlement (UE) 2016-679 – Règlement Général de Protection de Données.
2. En cas de contradictions, les dispositions de la présente convention avec toutes ses composantes priment sur les dispositions du contrat principal.
3. Par le terme "traitement des données" ou "traitement" (des données) utilisé dans le présent contrat, on entend la définition du "traitement" au sens de l'art. 4 n°2 du RGPD.
4. Le Sous-traitant s'engage à utiliser uniquement des « Data Center » dans les États membres de l'Union européenne (UE) ou de l'Espace économique européen (EEE) pour la fourniture du système de recrutement et de gestion des candidats.
5. Le transfert vers un pays tiers à des fins de mise à disposition conformément au paragraphe 4 ne peut avoir lieu que si les conditions particulières des art. 44 du RGPD et que le Client a donné son accord préalable à la délocalisation. Les dispositions du § 7 s'appliquent.

#### §2 Objet et durée du traitement

1. L'objet du présent accord est le traitement des données à caractère personnel par le Sous-traitant dans le cadre de l'utilisation du système de recrutement et de gestion des candidatures en tant que « Software as a Service » (SaaS) par le Client.
2. La nature, la portée et la finalité du traitement des données à caractère personnel pour le compte de l'entreprise sont précisées à **l'annexe 1** de la présente convention. Le traitement se fonde notamment sur les instructions du Client ainsi que sur l'étendue des produits fournis par le Sous-traitant, ses composants et le traitement effectué à ces fins.

## *Traduction libre*

### **Contrat de protection de données pour la sous-traitance en application de l'article 28 du RGPD**

3. Le Sous-traitant n'est autorisé à traiter des données qui s'écartent du traitement de la commande que s'il l'effectue en tant que propre responsable de son traitement au sens de l'art. 4 n° 7 du RGPD et identifie le traitement comme tel.
4. La durée du contrat de traitement dépend de la durée des relations contractuelles associées (contrats de service).

#### **§3 Droits et obligations du Client**

1. En tant que responsable du traitement au sens de l'art. 4 n° 7 du RGPD, le Client est responsable de la sauvegarde des droits des personnes concernées résultant des articles 12 à 23 du RGPD.
2. Le Client est responsable, dans le cadre du traitement effectué par le sous-traitant de la notification et du signalement en cas de violation de la protection des données personnelles prévus par les articles 33 et 34 du RGPD. Le Client est conscient que la communication du rapport sur la violation des données personnelles doit être faite à l'autorité de surveillance (CNIL) dans les 72 heures.
3. Le Client a le droit de donner des instructions au sous-traitant sur le type, la portée et la procédure de traitement des données. Les instructions verbales doivent être confirmées immédiatement par le Client sous forme écrite (au moins par e-mail/ticket).
4. Le Client s'engage à ne donner des instructions qu'aux personnes habilitées à les recevoir. Le sous-traitant est en droit d'assumer un pouvoir d'instruction correspondant dans le cas d'une instruction émise par le Client.
5. Nonobstant le paragraphe 4, le Client est en droit de nommer les personnes habilitées à donner des instructions au Sous-traitant.
6. Conformément au § 6 du présent accord, le Client est en droit de vérifier le respect des mesures techniques et organisationnelles du Sous-traitant.

#### **§4 Obligations du Sous-traitant**

1. En exécution du § 3 (2) de la présente convention, le Sous-traitant est tenu de notifier au Client et sans délai toute violation de la protection des données personnelles susceptible d'entraîner un risque pour les droits et libertés des personnes concernées et que le Sous-traitant traite pour le compte du Client.
2. Le rapport du Sous-traitant au Client doit contenir au moins les informations suivantes sur l'incident :
  - Une description de l'incident de violation des données personnelles ;
  - Des informations sur les données et les enregistrements des données affectées ainsi que sur l'étendue des personnes concernées ;

## **Traduction libre**

### **Contrat de protection de données pour la sous-traitance en application de l'article 28 du RGPD**

- Une évaluation préliminaire des conséquences probables de la violation des données à caractère personnel ;
  - Une description des mesures et/ou des propositions de mesures déjà prises par le sous-traitant pour éviter ou atténuer les conséquences négatives pour les personnes concernées.
3. Le Sous-traitant doit informer le Client sans délai si une autorité de contrôle prend des mesures à l'encontre du sous-traitant conformément à l'article 58 du RGPD et que cela concerne également le traitement effectué par le sous-traitant pour le compte du Client.
  4. En exécution du § 3 (1) du présent accord, le Sous-traitant informe immédiatement le Client si les personnes concernées font valoir leurs droits de personnes concernées contre le Sous-traitant. Le Sous-traitant s'engage à soutenir au mieux le Client dans le respect des droits des personnes concernées, en particulier selon les instructions du mandant et au moyen de mesures techniques et organisationnelles appropriées.
  5. Le Sous-traitant soutient le Client dans le respect des obligations visées aux articles 32 à 36 du RGPD, en tenant compte du type de traitement et des informations dont il dispose.
  6. Le Sous-traitant informe immédiatement le Client si, selon lui, une instruction donnée par le Client viole les dispositions légales. Le sous-traitant est en droit, sans reconnaître une obligation de vérifier l'existence d'une instruction illégale, de rejeter ou de suspendre une instruction illégale jusqu'à ce qu'elle soit confirmée ou modifiée par le Client ou de rejeter à tout moment des instructions manifestement illégales ou de suspendre le traitement qui y est lié.
  7. Le Sous-traitant désignera comme destinataire autorisé des instructions le département Service et support Client, contact : support@softgarden.de. Les employés de ce département ainsi que les responsables de secteur du sous-traitant sont habilités à recevoir des instructions.
  8. Conformément au § 9 de la présente convention, le Sous-traitant est tenu de respecter les mesures techniques et organisationnelles nécessaires au traitement.

#### **§5 Obligation de notification en cas de divulgation**

1. Le Sous-traitant informera immédiatement le Client de toute demande ou requête de divulgation d'informations de quelque nature que ce soit par les autorités de poursuite et autres organes gouvernementaux, dans la mesure où celles-ci sont en rapport avec les accords conclus entre le Client et le Sous-traitant ("Obligation de notifier").
2. Le Client est seul responsable de la décision et de la procédure de divulgation des informations concernées auprès des organismes gouvernementaux et doit aider le Sous-traitant au mieux de ses capacités dans cette divulgation.

**Contrat de protection de données pour la sous-traitance  
en application de l'article 28 du RGPD**

3. Le Sous-traitant n'est libéré de l'obligation d'informer le Client que s'il est lui-même tenu de divulguer des informations aux organismes gouvernementaux et de garder le secret vis-à-vis du Client.

**§6 Droit de contrôle du Client**

1. Le Client a le droit de procéder ou de faire procéder à des contrôles du respect des mesures techniques et organisationnelles par des auditeurs à désigner au cas par cas. Il a le droit de s'assurer, par le biais de contrôles aléatoires, notifiés au moins 14 jours à l'avance en raison du contrôle spécifique, du respect de la présente convention par le Sous-traitant dans le cadre de ses activités professionnelles pendant les heures normales de travail et en concertation avec le Sous-traitant.
2. Le Sous-traitant doit veiller à ce que le Client puisse s'assurer que les obligations du Sous-traitant en vertu de l'art. 28 du RGPD ont été respectées. Le Sous-traitant s'engage à fournir au Client les informations nécessaires sur demande et, en particulier, à prouver la mise en œuvre des mesures techniques et organisationnelles.
3. Les parties conviennent que les contrôles sur place au sens de l'al. 1 n'ont pas lieu plus d'une fois par an et ne sont nécessaires que si le respect des obligations du sous-traitant en vertu de l'art. 28 RGPD ne peut pas déjà être prouvé au moyen de preuves au sens du paragraphe 4. En outre, les inspections sur place doivent être justifiées par le Client en indiquant le contrôle spécifique et sont uniquement autorisées, pour plus d'un jour d'audit par an, dans des cas exceptionnels.
4. La preuve des mesures techniques et organisationnelles pour le respect des exigences particulières de la protection des données ainsi que de celles relatives à l'offre peut être apportée par :
  - des attestations, rapports ou extraits de rapports actuels émanant d'organismes indépendants (par exemple des auditeurs, des responsables de la protection des données, du service de sécurité informatique, des auditeurs de la protection des données, des auditeurs de la qualité) ;
  - une certification appropriée par un audit de sécurité informatique ou de protection des données.

Si d'autres preuves permettent au Client de s'assurer du respect des mesures techniques et organisationnelles conformément à l'annexe 2 du présent contrat, de manière appropriée et conforme aux exigences de protection, elles peuvent également être apportées (par ex. concepts, directives, états).

5. En cas de contrôle nécessaire (sur place) du Client chez le Sous-traitant, chaque partie supporte elle-même les frais occasionnés, tels que les frais de contrôle, de personnel et de déplacement. Dans la mesure où la collaboration du Sous-traitant dans le cadre des contrôles excède ce qui est nécessaire au sens du § 3 et que cela est lié à un effort

## Traduction libre

### Contrat de protection de données pour la sous-traitance en application de l'article 28 du RGPD

6. de contrôle plus important ou à la mise en œuvre de prestataires de services externes par le Sous-traitant (par ex. audit de plusieurs jours), les frais encourus à cet effet peuvent être facturés au Client conformément aux taux horaires et journaliers usuels dans le secteur.

#### §7 Relations de sous-traitance

1. Le Client accepte le recours aux sous-traitants visés à **l'annexe 1** sous la condition qu'un accord soit conclu avec lesdits sous-traitants conformément à l'art. 28 alinéa 2-4 du RGPD.
2. Le changement des sous-traitants existants conformément à **l'annexe 1** ou le recours à d'autres sous-traitants est autorisé aux conditions que :
  - Le Sous-traitant informe préalablement le Client de cette externalisation vers des sous-traitants par écrit ou sous une forme électronique appropriée, dans un délai raisonnable qui ne peut être inférieur à 14 jours,
  - le Client ne s'oppose pas au changement de sous-traitant prévu,
  - le Client ne s'oppose pas à l'externalisation prévue par écrit ou sous une forme électronique appropriée par le Sous-traitant au moment où les données sont remises,
  - un accord contractuel soit conclu conformément à l'art. 28 alinéa 2-4 du RGPD répondant au niveau de protection et de sécurité du traitement des données requis pour le traitement.
3. Les services optionnels et/ou gratuits de fournisseurs tiers ou de sous-traitants du Sous-traitant, qui peuvent généralement être utilisés par le Client par le biais d'une procédure dite "*opt-in*", ne constituent pas un droit légal au service en question ou à la fourniture spécifique du service. En particulier, le Sous-traitant se réserve le droit de désactiver ou de restreindre ces services en cas de raison significative.
4. Les services de prestataires tiers, qui peuvent être réservés via la « *place de marché* » du Sous-traitant et, dans la mesure du possible, individuellement et intégrés dans le système par le Sous-traitant au nom du Client, ne sont pas - sauf accord contraire - des sous-traitants du Sous-traitant et ne sont pas soumis à l'obligation de contrôle de la protection des données du Sous-traitant. En particulier, le Sous-traitant se réserve le droit de désactiver ou de restreindre ces services s'il existe une raison significative.

#### §8 Accord de confidentialité

1. Le Sous-traitant est tenu de maintenir la confidentialité des données personnelles qu'il traite et/ou dont il a connaissance dans le cadre des contrats de service.

**Contrat de protection de données pour la sous-traitance  
en application de l'article 28 du RGPD**

2. Le Sous-traitant doit sensibiliser ses employés avec les dispositions relatives à la protection des données qui les concernent et leur faire respecter la confidentialité des données personnelles traitées. Le Sous-traitant doit fournir une formation régulière sur la protection des données à destination des employés.

**§9 Mesures techniques et organisationnelles**

1. Le Sous-traitant s'engage, vis-à-vis du Client, à garantir les mesures techniques et organisationnelles nécessaires au respect des dispositions applicables en matière de protection des données. Cela inclut en particulier les exigences prévues par l'art. 32 du RGPD.
2. L'état des mesures techniques et organisationnelles existant au moment de la conclusion du contrat figure à **l'annexe 2** du présent accord. Les parties conviennent que des modifications de ces mesures techniques et organisationnelles peuvent être nécessaires afin de s'adapter aux circonstances techniques et juridiques.
3. Le Sous-traitant documente les modifications apportées aux mesures prises et les met à la disposition du Client à sa demande. Le Client a le droit de vérifier, ou de faire vérifier par un tiers expert, les mesures techniques et organisationnelles prises par le Sous-traitant. Les dispositions du § 6 de la présente convention sont applicables.
4. Le Sous-traitant publie et met régulièrement à jour les preuves du respect des mesures techniques et organisationnelles, conformément au § 6 de la présente convention, sur son site Internet, à sa discrétion et/ou en raison d'une autre obligation de publication du Sous-traitant.

**§10 Obligations du Sous-traitant après la cessation du contrat**

Après la cessation des contrats de service ou à la demande du Client - au plus tard à la cessation des contrats de service - le Sous-traitant doit restituer au Client l'ensemble des documents, données et résultats de traitement ou d'utilisation créés ainsi que les stocks de données en rapport avec la relation contractuelle, à sa discrétion et sur instruction du Client ou pour respecter les dispositions relatives à la protection des données personnelles. Il en va de même pour le matériel d'essai et de résidus. Les éventuelles obligations légales de conservation sont exclues de la suppression.

**§11 Responsabilité et dommages**

1. Le Client et le Sous-traitant sont responsables envers les personnes concernées conformément aux dispositions de l'article 82 du RGPD.
2. Si une personne concernée fait valoir des droits à des dommages et intérêts à l'encontre de l'un des partenaires contractuels pour violation des règles de protection

## *Traduction libre*

### **Contrat de protection de données pour la sous-traitance en application de l'article 28 du RGPD**

des données, la partie mise en cause doit en informer immédiatement l'autre partie.

3. Les parties s'entraident pour se défendre contre les demandes de dommages et intérêts des personnes concernées, à moins que cela ne compromette la position juridique d'une partie vis-à-vis de l'autre partie ou de l'autorité de contrôle.

#### **§ 12 Dispositions finales**

1. En cas de contradictions, les dispositions du présent accord ainsi que toutes ses composantes priment sur les dispositions du contrat principal associé.
2. Si une disposition du présent accord est ou devient invalide, cela n'affectera pas la validité de l'ensemble du contrat. Dans ce cas, sera réputé valable par un commun accord des parties, une disposition au plus proche du sens et de la signification économique de la disposition invalide.
3. Le présent contrat, ainsi que les modifications et les compléments au contrat, peuvent être conclus tant par écrit que sous une forme électronique appropriée. Les modifications ou compléments significatifs du présent contrat ne prennent effet que s'ils sont acceptés ou signés par la direction du sous-traitant.
4. Les annexes 1 et 2 du contrat en font partie intégrante.
5. Le droit de la République fédérale d'Allemagne s'applique exclusivement à la relation contractuelle et à son exécution. Pour tous les litiges découlant du présent contrat ou en rapport avec celui-ci, la clause attributive de juridiction du contrat principal s'applique dans la mesure où cela est autorisé.

*Traduction libre*

**Contrat de protection de données pour la sous-traitance  
en application de l'article 28 du RGPD**

**Annexe 1 : Précisions sur le contenu de l'offre**

**Annexe 2 : Mesures techniques et organisationnelles**

---

Lieu, Date

---

Lieu, Date

---

**Client**

Name/Signature/Cachet de l'entreprise

---

**Sous-traitants**

softgarden e-recruiting GmbH

## **Annexe 1 du contrat de protection de données en accord avec l'article 28 RGPD**

### **Concrétisation du traitement**

#### **1. Objet du traitement :**

L'objet de l'accord est le traitement des données personnelles par le logiciel de recrutement et de gestion des candidatures, y compris les composants du produit réservé et le traitement secondaire au sens large, qui sont traités pour le compte du Client.

#### **2. Type de traitement :**

" **Le traitement** " est basé sur la définition de l'art. 4 n° 2 du RGPD. Il comprend toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, par des moyens automatisés ou non, 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 mise en relation, la limitation, l'effacement ou la destruction.

#### **3. Finalités et spécification du traitement :**

Les principales finalités du traitement sont le recrutement et la gestion des candidats, y compris :

- la collecte et le recueil structurés des données relatives aux candidats ;
- la présentation structurée des données relatives aux candidats ;
- la communication avec les candidats, les recruteurs et les responsables RH ;
- la mise en œuvre et la communication avec des tiers et des partenaires de coopération ;
- l'évaluation des données relatives aux candidats sous la forme de rapports ;
- la mise à disposition d'un vivier de talents,
- la demande de commentaires de la part des candidats et des employés embauchés via le logiciel.

#### Catégories de personnes concernées :

Les groupes de personnes suivants sont concernés par le traitement des données effectué dans la commande :

- Candidat du Client ;
- Recruteurs, employés et responsables RH du Client ;
- Demandeurs d'emploi et candidats potentiels.

#### Catégories de données à caractère personnel

Les catégories suivantes de données personnelles des candidats peuvent être concernées :

- Informations personnelles : qualité, diplôme universitaire, prénom, nom de famille, nationalité, date de naissance, etc.
- Données de contact et d'adresse : rue, numéro de maison, code postal, ville, pays, état, numéro de téléphone, fax, adresse e-mail, etc.

## **Annexe 1 du contrat de protection de données en accord avec l'article 28 RGPD**

- Données de candidature : photo de la candidature, lettre de motivation, curriculum vitae, expérience professionnelle/références, diplômes (universitaires) et autres qualifications, classe du permis de conduire, souhait de voyager, etc.
- Données de compte et de connexion : compte du candidat, ID utilisateur, adresse IP, fichiers journaux.
- Données d'utilisation, si elles sont personnelles : contenu des courriels, invitations, réactions, critiques, etc.

Les catégories suivantes de données personnelles des recruteurs, des employés et des responsables RH, peuvent être concernées :

- Informations personnelles : qualité, diplôme universitaire, prénom, nom de famille, niveau fonctionnel, entreprise, etc.
- Données de contact et données d'adresse : siège de l'entreprise, numéro de téléphone, fax, adresse électronique, etc.
- Données de compte et de journal : ID de l'utilisateur, adresse IP, fichiers journaux, rôle, enregistrement du traitement dans le système, etc.
- Données d'utilisation : commentaires, contenu des e-mails, invitations, réactions, évaluations, etc.

### **Lieux de traitement des données**

Le traitement au nom de la commande a lieu aux endroits suivants :

#### **Softgarden e-recruiting GmbH (locaux commerciaux du sous-traitant).**

Site de Berlin : Tauentzienstraße 14, 10789 Berlin

Site de Sarrebruck : Europaallee 29, 66113 Saarbrücken

#### **MyLoc managed IT AG Am Gatherhof 44 40472 Düsseldorf (centre de données)**

Sites du prestataire de services : Am Gatherhof 44 40472 Düsseldorf ; Dans le Steele 40599 Düsseldorf

#### **PlusServer GmbH Welsersstraße 14 51149 Cologne (centre de données)**

Sites du prestataire de services : Dans la Steele 40599 Düsseldorf ; Welsestraße 14 51149 Cologne

#### **Equinix Germany GmbH, Kruppstraße, 60388 Frankfurt am Main (centre de données)**

Sites du prestataire de services : Rebstücker Straße 33, 60326 Frankfurt

### **Personnes recevant des instructions du sous-traitant**

Les personnes suivantes du sous-traitant sont autorisées à recevoir des instructions du Client : Équipe du service Clientèle : [support@softgarden.de](mailto:support@softgarden.de)

### **Responsable de traitement des données du Sous-traitant**

Le responsable de traitement des données collectées par le Sous-traitant est :

## Traduction libre

### Annexe 1 du contrat de protection de données en accord avec l'article 28 RGPD

Marco Tessendorf, procado Consulting, IT- & Medienservice GmbH, Warschauer Str. 58a, 10243 Berlin Contact : [ds-softgarden@procado.de](mailto:ds-softgarden@procado.de)

#### Sous-traitants autorisés

La confirmation du recours à des sous-traitants, ou à des services optionnels et/ou gratuits, s'effectue généralement via le système de recrutement par une procédure dite "opt-in" de l'utilisateur. Afin de ne pas rendre la mise à disposition et l'utilisation du logiciel dépendantes de services tiers, le Sous-traitant offrira également au Client la possibilité d'implémenter des services tiers dans le système pour le compte du Client, qui peuvent être réservés notamment via la place de marché du sous-traitant et - dans la mesure du possible - individuellement.

Nom et adresse du sous-traitant	Contenu de la demande
myLoc managed IT AG Am Gatherhof 44 D-40472 Dusseldorf	Colocation et services gérés.  Location de „racks“ et fourniture de :  <ul style="list-style-type: none"><li>- Pare-feu et répartiteurs de charge redondants ;</li><li>- Alimentation électrique redondante via un groupe électrogène de secours, des UPS (redondance n+1) et une alimentation A/B dans les racks de serveurs;</li><li>- Multiples connexions IP redondantes et infrastructure réseau redondante;</li><li>- réseaux de sauvegarde et d'administration séparés;</li><li>- refroidissement redondant et économe en énergie (redondance n+1);</li><li>- serveurs dédiés;</li><li>- Certificats SSL;</li><li>- remplacement du matériel serveur défectueux;</li><li>- autres activités d'assistance pour tous les systèmes de serveurs (par exemple, dans le cadre d'une surveillance proactive).</li></ul>
PlusServer GmbH Welserstraße 14 51149 Cologne	
Equinix (Germany) GmbH Rebstücker Straße 33 60326 Frankfurt/Main	Colocation et services gérés.
Textkernel B.V. Nieuwendammerkade 26a5 NL-1022 AB Amsterdam (Server location Germany)	Analyse de CV (optionnel Opt-In) :  <ul style="list-style-type: none"><li>- Convertir les CV téléchargés en un formulaire structuré ;</li><li>- Utilisation de l'IA pour la mise en correspondance des profils de candidature / offre d'emploi ;</li><li>- Services de maintenance et de support pour le service « CV-Parsing ».</li></ul>
Cronofy Ltd 9A Beck Street, Nottingham, NG1 1EQ, UK (Server location Germany)	Intégration du calendrier (option facultative) :  <ul style="list-style-type: none"><li>- pour organiser des réunions, des rendez-vous et des tâches ;</li><li>- traitement des structures de calendrier et des événements.</li></ul>

**Traduction libre**

**Annexe 1 du contrat de protection de données en accord avec l'article 28 RGPD**

<p>SBB Software und Beratung GmbH Bahnhofstrasse 7, 95119 Naila, Allemagne (site serveur Gunzenhausen, Allemagne)</p>	<p>Pitchyou (connexion WhatsApp) - Envoi d'une application via WhatsApp, activée dans le système JustHire. - Utilisation de la communication par messagerie via WhatsApp sans envoyer vos propres contacts de répertoire à WhatsApp.</p>
---	--

## Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD

### Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles décrites ci-dessous doivent être traitées de manière confidentielle. Elles ne doivent pas être reproduites en tout ou en partie ni transmises à des personnes non autorisées.

#### Abréviations :

- Data Center : centre de données
- B : siège Softgarten à Berlin
- SB : siège Softgarten à Saarbrücken

#### Confidentialité

#### Accès

Softgarten veille à ce que des personnes non autorisées n'aient pas accès aux bureaux, aux serveurs et aux salles d'archives. Ceci est réalisé par :

Mesures	ROW	B	SB	Notes
Zone de réception centrale	X	X	-	
Système d'alarme avec gardien de sécurité attaché	X	-	-	
Clés codées et remise des clés uniquement aux personnes autorisées	X	X	X	
Enregistrement des fermetures	X	X	X	
Définition et documentation des autorisations d'accès	X	X	X	
Documentation Accès aux personnes extérieures à l'entreprise (p. ex. personnel de maintenance, Clients, prestataires de services, partenaires, visiteurs, etc.)	X	X	X	
Entrée dans les locaux par des personnes extérieures à l'entreprise uniquement sous la direction d'un employé.	X	X	X	
Légitimation de l'accès autorisé (clé, PinCode)	X	X	X	
Authentification à deux facteurs lors de l'accès	X	-	-	
Retrait des moyens d'accès après expiration de l'autorisation	X	X	X	
Zones de sécurité avec différentes autorisations d'accès	X	X	X	

**Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD**

**Contrôle d'accès physique**

Softgarden empêche l'utilisation des systèmes informatiques par des personnes non autorisées. Ceci est fait par :

Mesures	ROW	B	SB	Notes
Mise en place d'un compte utilisateur par utilisateur	X	X	X	Utilisation de comptes de support personnels-indépendants pour l'accès aux systèmes des Clients, les données d'accès ne sont accessibles qu'aux employés autorisés
Authentification des personnes autorisées à traiter les données au moyen d'une procédure de mot de passe (avec caractères spéciaux, longueur minimale de huit caractères, changement régulier du mot de passe	X	X	X	
Stockage crypté des mots de passe	X	X	X	
Blocage automatique du compte utilisateur en cas de saisie multiple et incorrecte des données d'accès.	X	X	X	
Blocage automatique du poste de travail en cas d'inactivité	X	X	X	
Blocage immédiat des autorisations en cas de départ des employés (politique/instruction de travail)	X	X	X	
Contrôle régulier de la validité des autorisations	X	X	X	
Utilisation d'armoires verrouillables pour le stockage des dossiers papier	X	X	-	pas de stockage de dossiers papier dans le bureau de Sarrebruck
Transmission sécurisée des secrets d'authentification (credentials) dans le réseau en utilisant TLS/HTTPS, SSH, VPN (IPSec, openVPN)	X	X	X	
Blocage manuel des codes d'accès aux postes de travail en cas d'absence prolongée de l'employé correspondant (30 jours)	X	X	X	après le retour, les codes d'accès doivent être à nouveau déverrouillés manuellement par l'administration informatique
Restriction de l'accès au WLAN du bureau par un filtre d'adresses MAC	-	-	X	
Exploitation d'un WLAN de bureau pour les appareils mobiles et les visiteurs	-	X	X	

**Contrôle d'accès**

Softgarden garantit que les personnes autorisées à utiliser un système de traitement des données ne peuvent accéder qu'aux données faisant l'objet de leur autorisation d'accès, et que les données personnelles ne peuvent être lues, copiées, modifiées ou déplacées sans autorisation pendant leur traitement, leur utilisation et après leur stockage.

**Traduction libre**

**Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD**

Ceci est réalisé par :

Mesures	R O W	B	S B	Notes
Définition des autorisations d'accès aux données (création d'un concept d'autorisation)	X	X	X	
Stockage des données sur des supports de données cryptés	X			
Définition des pouvoirs de connaître, de saisir, de modifier et de supprimer les données traitées dans le cadre de l'exécution de la commande par le sous-traitant.	X	X	X	
Contrôle régulier des accès, des saisies, des modifications et des suppressions.	X	-	-	
Elimination des supports de données qui ne sont plus nécessaires (directive/ instructions de travail)	X	X	X	
Réglementation écrite pour la copie de données (politique de sécurité informatique / instructions de travail)	X	X	X	
Attribution d'autorisations minimales (principe du besoin de savoir)	X	X	X	
Pas d'attribution de mots de passe génériques Identifiants de groupe	X	-	-	Utilisation de comptes d'assistance personnels pour accéder aux systèmes des Clients, les données d'accès ne sont accessibles qu'aux employés autorisés.
Éviter la concentration des fonctions / la séparation des tâches des activités d'administration sur différentes personnes qualifiées.	X	X	X	
Conserver un historique des modifications administratives effectuées.	X	X	X	
Accès à l'infrastructure de production via VPN.	-	X	X	

**Contrôle de séparation**

Softgarden veille à ce que les données collectées à des fins différentes puissent être traitées séparément. Il n'est pas nécessaire de procéder à une séparation physique ; une séparation logique des données est suffisante. Ceci est réalisé par :

Mesures	ROW	B	SB	Notes
Identification des données enregistrées (lignes de fichier, ID, numéro de Client/transaction)	X	X	X	
Séparation logique des données traitées pour différents Clients Fonction ↯séparation/ production/ test	X	X	X	
Séparation logique des données personnelles des Clients respectifs par affectation aux comptes utilisateurs respectifs	X	X	X	Séparation des Clients du côté logiciel

**Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD**

**Intégrité**

**Commande de lecture**

Softgarden garantit que les données personnelles ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation pendant la transmission électronique ou pendant leur transport ou leur stockage sur des supports de données, et qu'il est possible de vérifier et de déterminer à quels endroits un transfert de données personnelles est envisagé au moyen d'un dispositif de transmission de données. Ceci est fait par :

Mesures	ROW	B	SB	Notes
Détermination des personnes autorisées à transmettre ou à transporter (électroniquement, manuellement)	X	X	X	
Contrôle de l'exhaustivité des données après le transport, la transmission et la transmission ou le stockage des données	X	X	X	Comparaison manuelle avec les sommes de contrôle
Mise en place de passerelles de sécurité aux points de transfert du réseau	X	X	X	
Utilisation d'une méthode de cryptage reconnue qui crypte toutes les communications entre le demandeur et les serveurs du sous-traitant.	X	X	X	
Les flux de données entrants et sortants sont filtrés par une solution moderne de pare-feu en cascade.	X	X	X	
Dans la mesure où des supports de données sont transmis par des entreprises de transport, les supports de données ne seront transmis qu'après authentification préalable par l'entreprise de transport.	X	X	X	
Les papiers et supports de données contenant des données personnelles sont éliminés par une entreprise d'élimination qualifiée, conformément aux dispositions relatives à la protection des données.	X	X	X	
L'effacement complet, conforme à la protection des données et permanent des supports de données contenant des données personnelles est consigné. Les journaux sont conservés à l'abri des contrôles pendant au moins 12 mois.	X	X	X	

**Contrôle de saisie**

Softgarden veille à ce qu'il soit possible de vérifier et de déterminer ultérieurement si et par qui des données personnelles ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données. Ceci est fait par :

## Traduction libre

### Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD

Mesures	ROW	B	SB	Notes
Documentation des autorisations d'accès (groupes d'accès aux instructions de travail et autorisation d'accès)	X	X	X	
Enregistrement des activités dans le cadre du contrat	X	X	X	
Contrôle aléatoire et évaluation des données du journal en cas d'utilisation abusive	X	-	X	Evaluation des fichiers log via l'équipe SysOps à Saarbrücken
Mise à disposition d'un historique pour tous les utilisateurs qui utilisent les programmes d'application correspondants pour le traitement des données à caractère personnel, qui enregistre quel utilisateur a effectué quelle action et quand, à condition que cette action modifie des données à caractère personnel.	X	X	X	Enregistrement de l'historique dans l'application " Just Hire ".

### Disponibilité et résilience

#### Contrôle de disponibilité

Softgarden garantit que les données personnelles sont protégées contre la destruction ou la perte accidentelle ou intentionnelle. Ceci est fait par :

Mesures	ROW	B	SB	Notes
Alimentation sans interruption (UPS)	X	X	X	
Protection antivirus (sur les postes)	X	X	X	Protection antivirus sur les postes de travail Windows
Protection antivirus (sur les serveurs)	X	X	X	
Pare-feu	X	X	X	
Plan d'urgence	X	X	X	
Centre de données géo-redondants	X	-	-	
Centrale d'alarme d'incendie	X	X	-	
Surveillance par monitoring	X	X	X	Surveillance 24h/24 et 7j/7 de tous les systèmes critiques grâce à des procédures de surveillance automatisées

#### Récupération de données

Softgarden garantit la capacité de rétablir rapidement la disponibilité des données personnelles et leur accès en cas d'incident physique ou technique en prenant les mesures suivantes :

Mesures	ROW	B	SB	Notes
Procédure de sauvegarde selon le concept de sauvegarde (quotidienne, hebdomadaire, mensuelle)	X	X	X	
Stockage des données de sauvegarde dans des armoires de sécurité des données, des coffres-forts, dans d'autres compartiments coupe-feu	X	X	X	

**Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD**

**Résilience**

Softgarden garantit la disponibilité et la résilience des systèmes critiques pour l'entreprise et des systèmes de traitement des données personnelles grâce aux mesures techniques et organisationnelles suivantes :

Mesures	ROW	B	SB	Notes
Virtualisation et fonctionnement dans une infrastructure de conteneurs avec des équilibres de charge.	X	-	-	
Tests de pénétration Fluke des produits Softgarden pour les vulnérabilités de sécurité.	X	-	-	Les produits Softgarden sont testés à proximité des centres de données. Non applicable à proximité des bureaux.  Des tests de pénétration par les Clients peuvent être effectués après consultation de softgarden sur l'environnement de mise en scène. L'exécution dans l'environnement de production n'est pas autorisée.

**Procédures de révision, d'évaluation et de contrôle périodiques**

Pour assurer le maintien et l'amélioration continue du niveau de protection des données et de la sécurité des informations, Softgarden se soumet régulièrement (au moins une fois par an) à des audits internes et externes.

Softgarden est certifié selon :

- DIN EN ISO 9001:2015
- DIN EN ISO/IEC 27001:2017, y compris les exigences des normes ISO/IEC 27017:2015 et ISO/IEC 27018:2019.

**Gestion de la protection des données et de la sécurité de l'information**

Softgarden garantit un processus d'examen et d'évaluation réguliers de l'efficacité des mesures de protection techniques et organisationnelles. Cela se fait par :

Mesures	ROW	B	SB	Notes
Information et obligation des employés de se conformer aux exigences de protection des données du RGPD	X	X	X	
Évaluation régulière du périmètre de protection des données par une équipe de protection des données	X	X	X	
Les tiers doivent soumettre une déclaration de confidentialité.	X	X	X	
S'il y a des chevauchements fonctionnels pour des raisons organisationnelles, le principe des quatre yeux est appliqué et documenté.	-	X	X	
Il existe une règle de représentation définie au sein des groupes de fonctions.	-	X	X	

## Traduction libre

### Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD

Mesures	ROW	B	SB	Notes
Examen régulier du système de gestion de la protection des données et de la sécurité de l'information par le biais d'audits internes et externes.	X	X	X	

### **Evaluation du niveau de protection adéquat (Art. 32 para. 2 RGPD)**

Softgarden assure une évaluation documentée d'un niveau de protection adéquat au regard des risques liés au traitement - notamment par la destruction, la perte, l'altération, la disclosure ou l'accès non autorisé - des données personnelles traitées pour le compte de l'entreprise. Cela se fait par :

Mesures	ROW	B	SB	Notes
Réaliser une analyse de risque pour le traitement des données personnelles	X	X	X	
Création de catégories d'exigences de protection	X	X	X	
Alignement des processus "Privacy by Design" et "Privacy Default"	-	X	X	
Réalisation d'analyses d'impact sur la protection des données (lorsque la loi l'exige)	X	X	X	

### **Contrôle des commandes (Art. 32 al. 3 et 4 RGPD)**

Softgarden garantit que les données personnelles traitées dans la commande ne seront traitées que conformément aux instructions du Client et pour la réalisation de l'objectif d'utilisation défini contractuellement. L'entrepreneur peut le prouver au moyen d'une procédure de certification conformément à l'art. 40 ou une procédure de certification approuvée conformément à l'art. 42 RGPD. S'il n'y a pas de certification, la preuve est apportée par :

Mesures	ROW	B	SB	Notes
Conception claire des contrats avec les sous-traitants	X	X	X	
Formalisation de la passation de commande (formulaires)	X	X	X	
Suivi régulier des activités	X	X	X	Suivi des processus softgarden via des audits internes
Les personnes autorisées du Client et les personnes autorisées à recevoir des instructions sont définies contractuellement, les instructions sont toujours faites sous forme de texte (e.B. par e-mail ou système de tickets).	X	X	X	
Softgarden informe immédiatement le Client des cas de perturbations opérationnelles graves, si des violations de la protection des données sont suspectées, si des erreurs sont détectées ou d'autres irrégularités dans le traitement des données du Client.	X	X	X	

**Traduction libre**

**Annexe 2 du contrat de protection de données en accord avec l'article 28 RGPD**

Mesures	ROW	B	SB	Notes
Les commandes sont saisies sous la forme d'un ticket d'assistance (informations minimales : Client/Client, action/commande partielle, spécification exacte des étapes/paramètres de traitement, processeurs, rendez-vous, destinataires le cas échéant), où le travail effectué est documenté. Il existe une association claire entre le numéro de ticket d'assistance et la commande Client.	X	X	X	

**Modifications des mesures techniques et organisationnelles**

Softgarden s'efforce de développer en permanence les mesures techniques et organisationnelles de protection des données personnelles. Il est garanti que les modifications du TOM n'entraînent pas une diminution du niveau de sécurité. Softgarden informera le Client des modifications importantes apportées au TOM.