ACCORD RELATIF AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL POUR LE COMPTE D'UN MANDANT

(traitement des données conformément à l'article 28 du RGPD)

entre

Entreprise

Adresse

ci-après dénommée « **le donneur d'ordre**

et

reev GmbH

Sandstr. 3

80335 Munich

ci-après **dénommé le prestataire**

1 Objet et durée de la commande

1.1 Le prestataire traite les données à caractère personnel pour le compte du client.

1.2 L'objet du contrat résulte de l'accord de prestation de services, qui prend effet à la signature du présent contrat et auquel il est fait référence ici (ci-après dénommé « accord de prestation »). Le contrat peut être complété par des commandes individuelles si nécessaire.

1.3 La durée de la présente commande correspond à la durée du contrat de prestation. Le présent accord sur le traitement des commandes fait automatiquement partie intégrante de toutes les commandes individuelles mentionnées au point 1, paragraphe 2, et les complète. Le présent accord prévaut sur les dispositions relatives à la protection des données des commandes individuelles.

2 Concrétisation du contenu de la commande

2.1 La nature et la finalité du traitement des données à caractère personnel par le mandataire pour le mandant sont décrites de manière concrète dans la convention de prestations du contrat de services ainsi que dans les offres/contrats correspondants qui en découlent.

2.2 Le traitement des données convenu dans le contrat est effectué exclusivement dans les États membres de l'Union européenne ou dans un autre État signataire de l'accord sur l'Espace économique européen. Tout transfert vers un pays tiers ne peut avoir lieu que si les conditions particulières prévues aux articles 44 et suivants du RGPD sont remplies.

Le niveau de protection approprié peut être assuré comme suit :

- par une décision d'adéquation de la Commission (art. 45, al. 3 du RGPD) ;
- par des règles internes contraignantes en matière de protection des données (art. 46, al. 2, let. b, en liaison avec l'art. 47 du RGPD) ;
- par des clauses types de protection des données (art. 46, al. 2, let. C et d RGPD) ;
- par des codes d' conduite approuvés (art. 46, al. 2, let. e, en liaison avec l'art. 40 du RGPD) ;
- par un mécanisme de certification approuvé (art. 46, al. 2, let. f en liaison avec l'art. 42 du RGPD).
- par d'autres mesures :

  Le contractant travaille exclusivement sur les systèmes mis à disposition par le client et ne stocke aucune donnée. (art. 46, al. 2, lit. a, al. 3, lit. a et b du RGPD).

2.3 Si nécessaire, une analyse d'impact relative au transfert de données est effectuée dans le cadre du traitement de données à caractère personnel dans des pays tiers non sûrs.

3 Type de données et groupes de personnes concernés

Les types/catégories de données suivants font l'objet du traitement des données à caractère personnel

Type de données	Finalité de la collecte, -traitement ou utilisation	Cercle des personnes concernées
Nom (prénom, nom) Adresse e-mail Numéro de téléphone (professionnel) - facultatif	Pour l'exécution du contrat : création d'un compte utilisateur et identification lors de la transmission du mot de passe	• Collaborateurs ayant accès à l'interface d'administration
Adresse e-mail, numéro de tag RFID, le cas échéant numéro de carte de recharge et nom de la carte	Pour l'exécution du contrat : création d'un compte utilisateur et identification lors de la transmission du mot de passe	• Collaborateurs en tant que conducteurs de VE • autres personnes (invités, sous-traitants) en tant que conducteurs de VE ; qui sont autorisées à utiliser régulièrement l'infrastructure de recharge
Nom, prénom Adresse (rue, numéro, code postal, ville)	Pour l'exécution du contrat : facturation des opérations de recharge effectuées	
Scan de la carte grise Coordonnées bancaires : • Titulaire du compte (nom, prénom) • IBAN	Pour l'exécution du contrat : traitement et facturation du commerce des quotas de réduction des gaz à effet de serre	• Employés conducteurs de véhicules électriques
Données relatives aux véhicules de société : • Numéro d'immatriculation • Numéro d'étiquette RFID • facultatif : fabricant, marque	Pour l'exécution du contrat : autorisation et attribution des opérations de chargement	• Propriétaires de véhicules de société du donneur d'ordre
Scan de la carte grise	Pour l'exécution du contrat : traitement du commerce des quotas de réduction des gaz à effet de serre	
Données relatives aux opérations de recharge : • Station de recharge et connexion, • Numéro d'étiquette RFID du conducteur ou du véhicule • Début et fin, • Énergie chargée, état du processus de recharge et puissance de recharge toutes les 5 minutes • Tarif	Pour l'exécution du contrat : autorisation, attribution et facturation des processus de recharge	• Employés en tant que conducteurs de VE • autres personnes (invités, sous-traitants) en tant que conducteurs de VE ; qui sont autorisées à utiliser régulièrement l'infrastructure de recharge • Propriétaires de véhicules de société du client

Données statistiques sur le comportement d'utilisation (anonymisées) : • utilisation de l'infrastructure de recharge – fréquence, quantité d'énergie et lieu par utilisateur		• Collaborateurs ayant accès à l'interface d'administration • Employés conducteurs de VE • autres personnes (invités, sous-traitants) en tant que conducteurs de VE ; qui sont régulièrement autorisées à utiliser l'infrastructure de recharge

4 Obligations du contractant

4.1 Mesures techniques et organisationnelles

4.1.1 Le contractant doit garantir la sécurité conformément à l'art. 28, al. 3, let. c, 32 RGPD, en particulier en liaison avec l'art. 5, al. 1, al. 2 RGPD. Dans l'ensemble, les mesures à prendre sont des mesures de sécurité des données et visent à garantir un niveau de protection adapté au risque en matière de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes. À cet égard, il convient de tenir compte de l'état de la technique, des coûts de mise en œuvre, de la nature, de la portée et des finalités du traitement, ainsi que de la probabilité et de la gravité du risque pour les droits et libertés des personnes physiques au sens de l'article 32, paragraphe 1, du RGPD.

4.1.2 Les mesures techniques et organisationnelles sont soumises au progrès technique et à l'évolution. À cet égard, le contractant est autorisé à mettre en œuvre des mesures alternatives adéquates. Le niveau de sécurité des mesures définies ne doit toutefois pas être réduit. Les modifications importantes doivent être documentées.

4.1.3 Le résumé des mesures techniques et organisationnelles actuelles du contractant est joint en **annexe** au présent accord, auquel le client déclare donner son accord.

4.2 Obligation d'assistance

4.2.1 Lors de l'exercice des droits des personnes concernées conformément aux articles 12 à 22 du RGPD par le client, lors de l'établissement du registre des activités de traitement du client et lors du respect des obligations en matière de sécurité des données à caractère personnel énoncées aux articles 32 à 36 du RGPD, obligations de notification en cas de violation des données, évaluations de l'impact sur la protection des données et consultations préalables, le prestataire doit coopérer dans la mesure nécessaire et assister le client de manière appropriée dans la mesure du possible. Il doit transmettre sans délai au client les informations nécessaires à cet effet. Cela comprend notamment

4.2.1.1 la garantie d'un niveau de protection approprié par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement ainsi que de la probabilité et de la gravité prévisibles d'une violation potentielle résultant de lacunes en matière de sécurité et qui permettent une détection immédiate des violations pertinentes

4.2.1.2 l'obligation de signaler immédiatement toute violation des données à caractère personnel au client

4.2.1.3 l'obligation d'assister le donneur d'ordre dans le cadre de son obligation d'information envers la personne concernée et de lui fournir sans délai toutes les informations pertinentes à cet égard

4.2.1.4 l'assistance du client dans le cadre de son analyse d'impact relative à la protection des données

4.2.1.5 l'assistance du client dans le cadre de consultations préalables avec l'autorité de contrôle

4.2.1.6 fournir immédiatement les informations nécessaires

4.2.1.7 le soutien du client dans le cadre de son analyse d'impact relative à la protection des données

4.2.1.8 le soutien du donneur d'ordre dans le cadre de consultations préalables avec l'autorité de contrôle

4.2.2 Pour les prestations d'assistance qui ne sont pas incluses dans la description des prestations ou qui ne sont pas imputables à une faute du contractant et qui vont au-delà des obligations légales du contractant, le contractant peut exiger une rémunération appropriée. En ce qui concerne le montant de la rémunération, il est renvoyé à la clause de rémunération correspondante.

4.3 Traitement des données à caractère personnel à domicile ou dans un bureau mobile

4.3.1 Le client accepte le traitement des données en dehors des locaux de l'entreprise (par exemple, télétravail, travail à domicile, bureau à domicile, travail mobile). Le contractant s'engage :

4.3.2 à aider ses employés à respecter les mesures techniques et organisationnelles nécessaires dans leurs locaux privés afin de garantir la sécurité des données.

4.3.3 à informer de manière appropriée ses employés sur le respect des mesures techniques et organisationnelles et des autres obligations de diligence à respecter lors du traitement des données dans des locaux privés.

5 Autres obligations du contractant

5.1 Le contractant garantit la désignation par écrit d'un délégué à la protection des données qui exerce ses fonctions conformément aux articles 38 et 39 du RGPD.

5.2 Le contractant garantit la mise à disposition d'un délégué à la protection des données :

Le délégué à la protection des données désigné chez le prestataire est SiDIT GmbH,info@sidit.de , Tél. : +49 931 78 08 77 - 0. Tout changement de délégué à la protection des données sera indiqué dans la déclaration de confidentialité.

5.3 Le contractant garantit le respect de la confidentialité conformément à l'art. 28, al. 3, phrase 2, let. b, 29 et 32, al. 4 du RGPD. Le contractant n'emploie pour l'exécution des travaux que des collaborateurs qui sont tenus à la confidentialité et qui ont été préalablement informés des dispositions relatives à la protection des données qui les concernent. Le contractant et toute personne subordonnée au contractant qui a accès à des données à caractère personnel ne peuvent traiter ces données que conformément aux instructions du donneur d'ordre, y compris les pouvoirs accordés dans le présent contrat, à moins qu'ils ne soient légalement tenus de les traiter. Cette obligation de confidentialité des employés reste en vigueur même après la fin de leur contrat de travail respectif.

5.4 Le donneur d'ordre et le prestataire coopèrent, sur demande, avec l'autorité de contrôle dans l'exercice de ses fonctions.

5.5 Le contractant garantit d'informer immédiatement le donneur d'ordre des contrôles et mesures effectués par l'autorité de contrôle dans la mesure où ils se rapportent à la présente commande. Cela s'applique également dans la mesure où une autorité compétente mène une enquête dans le cadre d'une procédure administrative ou pénale relative au traitement de données à caractère personnel dans le cadre du traitement des commandes chez le contractant.

5.6 Dans la mesure où le donneur d'ordre fait lui-même l'objet d'un contrôle de l'autorité de contrôle, d'une procédure pour infraction administrative ou pénale, d'une action en responsabilité d'une personne concernée ou d'un tiers ou de toute autre action en rapport avec le traitement des données chez le preneur d'ordre

, le contractant doit l'assister au mieux de ses capacités. Le contractant peut exiger une rémunération appropriée pour les prestations d'assistance qui ne sont pas incluses dans la description des prestations, qui ne sont pas imputables à un comportement fautif du contractant et qui vont au-delà des obligations légales du contractant.

5.7 Le contractant contrôle régulièrement les processus internes ainsi que les mesures techniques et organisationnelles afin de garantir que le traitement relevant de sa responsabilité est conforme aux exigences de la législation applicable en matière de protection des données et que la protection des droits de la personne concernée est garantie.

6 Obligations et droits du client

6.1 Responsabilité

6.1.1 Le donneur d'ordre est seul responsable de l'évaluation de la licéité du traitement conformément à l'article 6, paragraphe 1, du RGPD et du respect des droits des personnes concernées conformément aux articles 12 à 22 du RGPD. Néanmoins, le preneur d'ordre est tenu de transmettre sans délai au donneur d'ordre toutes les demandes de ce type, dans la mesure où elles sont manifestement adressées exclusivement au donneur d'ordre.

6.1.2 Toute modification de l'objet du traitement et toute modification des procédures doivent être convenues conjointement entre le donneur d'ordre et le prestataire et consignées par écrit ou dans un format électronique documenté.

6.2 Pouvoir de donner des instructions

6.2.1 Le contractant ne traite les données à caractère personnel que sur la base d'instructions documentées du donneur d'ordre, à moins qu'il ne soit tenu de le faire en vertu du droit d'un État membre ou du droit de l'Union. Le donneur d'ordre confirme immédiatement les instructions verbales (au moins sous forme écrite). Les instructions initiales du donneur d'ordre sont fixées dans le présent contrat.

6.2.2 Le contractant ne peut pas rectifier, supprimer ou limiter le traitement des données traitées dans le cadre de la commande de sa propre initiative, mais uniquement sur instruction documentée du donneur d'ordre. Si une personne concernée s'adresse directement au prestataire à ce sujet, celui-ci transmettra immédiatement cette demande au donneur d'ordre. Si cela est techniquement possible et nécessaire au regard de l'objet du contrat de prestation, le prestataire peut également supprimer des données de dispositifs sans instruction à cet effet (par exemple en cas de remplacement rapide et techniquement nécessaire d'un

appareil). Si la suppression des données entraîne des frais pour le mandataire, ceux-ci sont à la charge du mandant.

6.2.3 Le mandataire doit informer immédiatement le mandant s'il estime qu'une instruction enfreint les dispositions en matière de protection des données. Le mandataire est en droit de suspendre l'exécution de l'instruction correspondante jusqu'à ce qu'elle soit confirmée ou modifiée par le mandant.

6.2.4 Aucune copie ou duplication des données n'est effectuée à l'insu du client. Font exception à cette règle les copies de sécurité nécessaires pour garantir un traitement correct des données, ainsi que les données requises pour respecter les obligations légales de conservation.

6.3 Droits de contrôle

6.3.1 Le client a le droit, en concertation avec le prestataire, de procéder à des contrôles visant à vérifier le respect des dispositions relatives à la protection et à la sécurité des données ainsi que des accords contractuels dans une mesure appropriée et nécessaire, ou de les faire effectuer par des contrôleurs désignés au cas par cas. Le prestataire est libre de présenter au client, afin de satisfaire à ce droit de contrôle, des rapports de contrôle ou des documents similaires attestant que le traitement des données est conforme à la protection des données. Si le donneur d'ordre a des doutes quant à la conformité du traitement des données avec la protection des données, il a le droit de s'assurer du respect du présent accord par le preneur d'ordre dans le cadre de ses activités commerciales au moyen de contrôles aléatoires, qui doivent généralement être annoncés en temps utile.

6.3.2 Le prestataire veille à ce que le client puisse s'assurer du respect des obligations du prestataire conformément à l'article 28 du RGPD. Le prestataire s'engage à fournir au client, sur demande, les informations nécessaires et, en particulier, à prouver la mise en œuvre des mesures techniques et organisationnelles.

6.3.3 Le contractant est en droit de fournir la preuve de telles mesures qui ne concernent pas uniquement la commande concrète, par

6.3.3.1 le respect des règles de conduite approuvées conformément à l'article 40 du RGPD ;

6.3.3.2 la certification selon une procédure de certification approuvée conformément à l'article 42 du RGPD ;

6.3.3.3 des attestations, rapports ou extraits de rapports récents émanant d'instances indépendantes (par exemple, experts-comptables, réviseurs, délégués à la protection des données, service de sécurité informatique, auditeurs de protection des données, auditeurs qualité) ;

6.3.3.4 une certification appropriée par un audit de sécurité informatique ou de protection des données (par exemple, conformément à la protection de base du BSI).

6.3.4 Le contractant peut faire valoir un droit à rémunération pour permettre au donneur d'ordre d'effectuer des contrôles. La facturation des frais engagés selon les taux horaires habituellement demandés par le contractant est considérée comme raisonnable.

7 Sous-traitance

7.1 Au sens de la présente réglementation, on entend par sous-traitance les prestations qui se rapportent directement à la fourniture de la prestation principale. Ne sont pas comprises les prestations accessoires fournies par le contractant, par exemple les prestations de télécommunication, les /de transport, de maintenance et d'assistance aux utilisateurs ou l'élimination de supports de données, ainsi que d'autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des systèmes de traitement des données. Le contractant est toutefois tenu de prendre des mesures contractuelles et de contrôle appropriées et conformes à la loi afin de garantir la protection et la sécurité des données du client, même en cas de sous-traitance de prestations accessoires.

7.2 L'externalisation à des sous-traitants ou le changement de sous-traitant existant sont autorisés dans la mesure où le prestataire informe le client par écrit ou sous forme de texte au moins quatre semaines avant le changement prévu et où le client ne s'oppose pas par écrit ou sous forme de texte à l'externalisation prévue dans un délai de deux semaines à compter de la réception de la notification du prestataire. Le contractant conclura avec le sous-traitant un accord contractuel conformément à l'article 28, paragraphes 2 à 4, du RGPD. Si le client refuse son consentement pour des raisons autres que des raisons importantes, le contractant peut résilier le contrat à la date prévue pour l'intervention du sous-traitant.

7.3 Le donneur d'ordre accepte la sous-traitance aux sous-traitants suivants sous réserve d'un accord contractuel conformément à l'article 28, paragraphes 2 à 4 du RGPD :

Nom et adresse du sous-traitant	**Description des prestations partielles**
AWS - Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 États-Unis	Hébergement de serveurs (Europe)

7.4 La transmission des données à caractère personnel du donneur d'ordre au sous-traitant et la première intervention de ce dernier ne sont autorisées qu'une fois toutes les conditions préalables à la sous-traitance remplies.

7.5 Si le sous-traitant fournit la prestation convenue en dehors de l'UE/EEE, le prestataire garantit la conformité avec la législation sur la protection des données en prenant les mesures appropriées. Il en va de même lorsque des prestataires de services au sens de l'alinéa 1, phrase 2, doivent être utilisés.

8 Suppression et restitution des données à caractère personnel

8.1 Après l'achèvement des travaux convenus dans le contrat ou plus tôt à la demande du donneur d'ordre, au plus tard à la fin du contrat de prestation, le preneur d'ordre doit remettre au donneur d'ordre tous les documents en sa possession, les résultats du traitement et de l'utilisation ainsi que les bases de données en rapport avec la relation contractuelle, ou les détruire conformément à la protection des données après accord préalable. Il en va de même pour le matériel de test et les rebuts. Le procès-verbal de suppression doit être présenté sur demande. Si le prestataire engage des frais pour la remise ou la suppression des données, ceux-ci sont à la charge du client.

8.2 Les documents servant à prouver le traitement correct et conforme des données doivent être conservés par le prestataire au-delà de la fin du contrat, conformément aux délais de conservation applicables. Il peut les remettre au client à la fin du contrat pour se décharger de cette obligation.

9 Responsabilité et dommages-intérêts

9.1 Le donneur d'ordre garantit, dans son domaine de responsabilité, la mise en œuvre des dispositions légales applicables en matière de traitement des données à caractère personnel.

9.2 Les limitations de responsabilité prévues dans le contrat principal s'appliquent en principe. Le donneur d'ordre dégage le preneur d'ordre de toute responsabilité vis-à-vis de tiers qui font valoir des droits à l'encontre du preneur d'ordre en raison d'une violation de leurs droits résultant du traitement de données à caractère personnel commandé par le donneur d'ordre, sauf si la revendication du tiers repose sur un traitement illicite des données à caractère personnel par le preneur d'ordre. L'article 82 du RGPD reste inchangé.

10 Divers, généralités

10.1 Si les données à caractère personnel du donneur d'ordre sont menacées chez le preneur d'ordre par saisie ou confiscation, par une procédure d'insolvabilité ou de concordat ou par d'autres événements ou mesures de tiers, le preneur d'ordre doit en informer immédiatement le donneur d'ordre

en informer immédiatement. Le prestataire informera immédiatement toutes les personnes responsables dans ce contexte que la souveraineté sur les données à caractère personnel du client appartient au client.

10.2 Les dispositions du présent accord restent en vigueur après la fin de la relation contractuelle initiale jusqu'à la destruction complète ou la restitution au client de toutes les données à caractère personnel du client.

10.3 Si certaines parties du présent accord sont invalides, cela n'affecte pas la validité du reste de l'accord. Les parties s'engagent à remplacer la disposition invalide par une disposition légale qui se rapproche le plus possible de l'objectif de la disposition invalide.

_____	_____
Lieu, date	Signature du client
_____	_____
Lieu, date	Signature du mandataire

(Révisé en octobre 2024)

Annexe 1 à
l'accord AV :

Mesures techniques et organisationnelles

conformément à l'art. 32, al. 1 du RGPD

1. Confidentialité (art. 32, al. 1, let. b) du RGPD)

1.1. Contrôle de l'accès

Toutes les mesures visant à empêcher l'accès des personnes non autorisées aux installations de traitement des données à caractère personnel sont énumérées ci-dessous :

- Système de sonnette avec caméra
- Cartes à puce / systèmes de transpondeurs
- Portes avec poignée à l'extérieur
- Règlement relatif aux clés / registre des clés
- Règlement relatif à la délivrance des badges
- Règlement pour la remise des jetons
- Visiteurs / personnes externes accompagnées par des collaborateurs
- Service de nettoyage externe
- Service de maintenance externe
- Mesures à prendre en cas de perte de clés / badges / dongles / jetons / cartes à puce

1.2. Contrôle d'accès

Toutes les mesures visant à empêcher l'accès non autorisé aux systèmes de traitement des données sont énumérées ci-dessous :

- Connexion avec nom d'utilisateur+ mot de passe
- Connexion avec données biométriques
- Logiciels antivirus Clients
- Pare-feu - Serveur
- Accès externe via mobile / bureau à domicile (par exemple PC / ordinateur portable)
- Accès externe par des prestataires externes
- Accès externe via smartphones/tablettes
- Cryptage des supports de données
- Verrouillage automatique des ordinateurs
- Cryptage des ordinateurs portables / tablettes
- Cryptage lors de l'utilisation du Wi-Fi (WPA2)
- Création et gestion des profils utilisateur et des autorisations
- Instructions « Verrouillage manuel du bureau »
- Politique « Mot de passe sécurisé »
- Politique « Suppression / Destruction »
- Directive « Bureau propre »
- Directive « Bureau à domicile/mobile »
- Politique relative aux appareils mobiles

1.3. Contrôle d'accès

Toutes les mesures visant à empêcher toute personne non autorisée de lire, copier, modifier ou supprimer des données dans les systèmes de traitement des données sont énumérées ci-dessous :

- Destructeur de documents
- Destructeur de documents externe
- Suppression physique des supports de données
- Concept(s) d'autorisation

- Nombre minimal d'administrateurs
- Coffre-fort pour la protection des données
- Gestion des droits d'utilisateur par les administrateurs

1.4. Contrôle de la séparation

Toutes les mesures visant à séparer les données à caractère personnel collectées à des fins différentes sont énumérées ci-dessous :

- Séparation des environnements de production et de test
- Séparation physique (systèmes / bases de données / supports de données)
- Capacité multi-clients des applications concernées
- Autorisations d'accès des collaborateurs adaptées aux besoins
- Définition des droits d'accès aux bases de données

1.5. Pseudonymisation (Art. 32, al. 1, let. a) et art. 25, al. 1 du RGPD)

La pseudonymisation des ensembles de données est mise en œuvre par les mesures suivantes :

Il n'y a pas de pseudonymisation des ensembles de données.

2. Intégrité (art. 32, al. 1, let. b) RGPD)

2.1. Contrôle de la transmission

Les données à caractère personnel doivent être protégées de manière adéquate lors de leur transmission électronique afin d'empêcher toute lecture, copie, modification ou suppression non autorisée. Nous avons pris les mesures techniques et organisationnelles suivantes à cet effet :

- Cryptage des e-mails
- Mise à disposition de connexions tunnel (VPN)
- Mise à disposition de connexions cryptées
- Procédures de signature électronique
- Enregistrement des accès et des consultations dans des fichiers journaux
- Sélection rigoureuse du personnel de transport et des véhicules

2.2. Contrôle des entrées

Afin de contrôler si et par qui des données à caractère personnel sont saisies, modifiées, bloquées ou supprimées dans le système de traitement des données, nous mettons en œuvre les mesures suivantes :

- Enregistrement technique de la saisie, de la modification et de la suppression des données
- Contrôle manuel ou automatisé des protocoles
- Liste des logiciels avec programmes de traitement des données
- Attribution de noms d'utilisateur individuels
- Concept d'autorisation avec attribution de droits d'utilisateur adaptés aux besoins
- Conservation sécurisée des documents papier

3. Disponibilité et résilience (art. 32, al. 1, let. b) RGPD)

3.1. Contrôle de la disponibilité

Afin de garantir la disponibilité des données à caractère personnel contre la destruction accidentelle ou intentionnelle ou la perte, nous mettons en œuvre les mesures suivantes :

- Conservation des supports de sauvegarde dans un endroit sûr en dehors de la salle des serveurs
- Partitions séparées pour les systèmes d'exploitation et les données

Nous garantissons le rétablissement rapide de la disponibilité (art. 32, al. 1, let. c) du RGPD) grâce aux mesures suivantes :

4. Procédures de surveillance régulière, appréciation et évaluation (art. 32, al. 1, let. d) du RGPD et art. 25, al. 1 du RGPD)

Date de l'évaluation des mesures techniques et organisationnelles :

- 17/11/2022

4.1. Gestion de la protection des données

Afin de garantir la protection des données dans notre entreprise, nous mettons en œuvre les mesures suivantes pour contrôler, évaluer et analyser régulièrement :

- Solutions logicielles utilisées pour la gestion de la protection des données
- Documentation centralisée de toutes les procédures et réglementations relatives à la protection des données, accessible aux employés
- Une vérification de l'efficacité des mesures techniques de protection est effectuée au moins une fois par an
- Délégué externe à la protection des données : Iris Duch, SiDIT GmbH, info@sidit.de
- Responsable interne de la sécurité de l'information : José Carvalho, reev GmbH, josé.carvalho@reev.com
- Employés formés et tenus au secret professionnel / à la confidentialité des données
- Sensibilisation régulière des collaborateurs au moins une fois par an
- Une analyse d'impact relative à la protection des données (AIPD) est réalisée si nécessaire
- L'organisation respecte les obligations d'information prévues aux articles 13 et 14 du RGPD
- Processus formalisé pour le traitement des demandes d'accès, de suppression et de transfert des données par les personnes concernées

4.2. Gestion des incidents (conformément à l'article 33 du RGPD)

En cas de détection et de signalement de violations de la protection des données, nous mettons en œuvre les mesures suivantes :

- Utilisation d'un pare-feu et mise à jour régulière
- Utilisation d'un filtre anti-spam et mise à jour régulière
- Utilisation d'un antivirus et mise à jour régulière
- Processus documenté pour la détection et la notification des incidents de sécurité / violations de données
- Procédure documentée pour le traitement des incidents de sécurité
- Implication du DSB dans les incidents de sécurité et les violations de données
- Implication de l'ISB dans les incidents de sécurité et les violations de données
- Documentation des incidents de sécurité et des violations de données
- Processus formel et responsabilités pour le suivi des incidents de sécurité et des violations de données

4.3. Paramètres par défaut respectueux de la protection des données

Dans le cadre des paramètres par défaut respectueux de la protection des données (art. 25, al. 2 du RGPD), nous mettons en œuvre les mesures suivantes :

- Minimisation des données et limitation de la finalité
- Exercice (technique) simple du droit de rétractation de la personne concernée grâce à des mesures techniques

4.4. Contrôle des commandes (externalisation)

Dans le cadre de l'externalisation du traitement des données à caractère personnel par des sous-traitants, nous mettons en œuvre les mesures suivantes afin de garantir un niveau de protection adéquat :

- Vérification préalable des mesures de sécurité prises par le sous-traitant et documentation de celles-ci
- Sélection du sous-traitant selon des critères de diligence (notamment en matière de protection et de sécurité des données)
- Conclusion de l'accord nécessaire pour le traitement des commandes ou des clauses contractuelles types de l'UE
- Instructions écrites au sous-traitant
- Obligation de confidentialité des données pour les collaborateurs du mandataire
- Obligation pour le contractant de désigner un délégué à la protection des données lorsque cette obligation existe
- Convention de droits de contrôle efficaces à l'égard du contractant
- Réglementation relative au recours à d'autres sous-traitants
- Garantie de la destruction des données après l'exécution de la commande
- En cas de collaboration de longue durée : contrôle régulier du contractant et de son niveau de protection