# Conditions d'utilisation

## Conditions d'utilisation

Conditions d'utilisation de la surveillance des réfrigérateurs apotec®.

L'objet de ces conditions d'utilisation est le service de surveillance de réfrigérateurs de WEPA APOTHEKENBEDARF GmbH & Co. KG (ci-après « WEPA ») mis à disposition par apotec® surveillance de réfrigérateurs (ci-après « apotec® surveillance de réfrigérateurs »).

**1. Domaine d'application**

1.1 Les conditions d'utilisation suivantes s'appliquent exclusivement à l'utilisation d'apotec® Surveillance de réfrigérateurs. Le fournisseur de la surveillance de réfrigérateurs est la société WEPA APOTHEKENBEDARF GmbH & Co. KG, Am Fichtenstrauch 6-10, 56204 Hillscheid, représentée par le gérant Dr. Christian Ciesielski.

1.2 apotec® Kühlschranküberwachung s'adresse exclusivement aux utilisateurs qui agissent dans l'exercice de leur activité professionnelle commerciale ou indépendante. Les autres utilisateurs, en particulier les consommateurs au sens du paragraphe 13 du Code civil allemand (BGB), sont exclus de l'utilisation d'apotec® Surveillance des réfrigérateurs.

**2. Objet d'apotec® Surveillance des réfrigérateurs**

2.1 apotec® surveillance de réfrigérateurs est un service numérique basé sur cloud qui permet d'enregistrer l'état de commutation des composants ainsi que les états d'alarme et les températures d'un ou plusieurs réfrigérateurs et congélateurs professionnels et de les représenter visuellement dans une application basée sur un navigateur. En outre, la surveillance des réfrigérateurs permet d'enregistrer et de représenter des grandeurs de mesure au moyen de capteurs externes, qui peuvent être achetés en différentes variantes comme accessoires du système de surveillance des réfrigérateurs apotec®.

**3. Droit d'utilisation**

3.1 Conformément aux présentes conditions d'utilisation, l'utilisateur est exclusivement autorisé par WEPA à utiliser le système de surveillance de réfrigérateurs apotec®. Le droit d'utilisation est un droit d'utilisation simple, non exclusif, non transmissible et limité dans le temps conformément au point 5.1 (ci-après « licence apotec® Kühlschranküberwachung »)

**4. Conditions d'utilisation et obligations de l'utilisateur**

4.1 Pour pouvoir utiliser apotec® Surveillance des réfrigérateurs, l'utilisateur a besoin, à ses frais :

· d'un réfrigérateur et/ou d'un congélateur adapté à la surveillance de réfrigérateur apotec®,

· d'une fiche RS485 et d'un adaptateur RS485 pour la mise en réseau du réfrigérateur et/ou du congélateur,

· d'une licence apotec® surveillance de réfrigérateur valable pour le réfrigérateur et/ou le congélateur concerné et

· d'un compte WEPA actif.

4.2 L'utilisateur s'engage à n'enregistrer que des réfrigérateurs et/ou congélateurs autorisés par WEPA pour la surveillance de réfrigérateurs apotec® et à tenir à jour ses données de contact dans le profil d'utilisateur de la surveillance de réfrigérateurs apotec®.

4.3 La surveillance de réfrigérateur apotec® ne peut être utilisée qu'avec des réfrigérateurs et/ou congélateurs agréés par WEPA pour la surveillance de réfrigérateur apotec® et installés et utilisés dans l'Union européenne, les pays de l'AELE ou le Royaume-Uni.

4.4 Les réfrigérateurs et/ou congélateurs approuvés par WEPA pour la surveillance des réfrigérateurs apotec® ne peuvent être mis en réseau qu'avec les solutions de mise en réseau approuvées par WEPA.

4.5 L'utilisateur ne doit pas utiliser apotec® Surveillance de réfrigérateur de manière abusive, en particulier il ne doit pas contourner les restrictions techniques d'apotec® Surveillance de réfrigérateur ou poursuivre des objectifs contraires à la loi.

**5. Durée du contrat**

5.1 Le contrat débute avec l'activation de la clé de licence dans l'apotec® Surveillance des réfrigérateurs et présente, selon l'abonnement choisi, une durée contractuelle de 12 ou 36 mois. La durée du contrat applicable à l'utilisateur dans un cas particulier est indiquée dans la confirmation de commande. Il se prolonge à chaque fois de la durée susmentionnée s'il n'est pas résilié avec un préavis de quatre semaines avant la fin du contrat.

5.2 La possibilité d'une résiliation sans préavis pour motif grave reste inchangée. Un motif important autorisant WEPA à résilier sans préavis existe notamment lorsque

5.2.1 l'utilisateur viole les droits d'utilisation de WEPA en utilisant la surveillance des réfrigérateurs apotec® audelà de ce qui est autorisé par les présentes conditions d'utilisation ou les conditions de licence à conclure également et qu'il ne met pas fin à la violation dans un délai raisonnable après un avertissement de WEPA ;

5.2.2 l'utilisateur est en retard de deux mois ou plus dans le paiement de la rémunération due ;

5.2.3 l'utilisateur subit ou risque de subir des pertes importantes dans sa situation économique, en particulier si le client lui-même demande l'ouverture d'une procédure d'insolvabilité sur ses biens ou si une procédure d'insolvabilité est ouverte sur ses biens.

5.2.4 si le partenaire de coopération Liebherr-Hausgeräte Vertriebs- und Service GmbH ne fournit plus à WEPA les prestations convenues avec WEPA (par ex. en raison de la résiliation de la relation contractuelle) et que WEPA ne peut donc plus proposer la prestation due.

5.3 Pour être valables, les déclarations de résiliation doivent revêtir la forme écrite. Le respect de cette forme est une condition préalable à la validité de la résiliation.

5.4 A la fin du contrat, WEPA désactivera le service dans le Cloud WEPA et supprimera les droits d'accès de l'utilisateur au service.

**6. Rémunération de l'utilisation**

6.1 La rémunération à payer par l'utilisateur est indiquée dans la confirmation de la commande. Tous les prix s'entendent en EUR, TVA légale en sus.

6.2 Les modalités de paiement sont indiquées dans la confirmation de la commande.

6.3 WEPA peut adapter la redevance d'utilisation selon le point 6.1 en toute équité (§ 315 al. 3 BGB) à l'évolution des coûts qui sont déterminants pour le calcul du prix. Sont notamment déterminantes pour le calcul du prix les redevances de licence que WEPA doit verser pour l'exploitation du système de surveillance de réfrigérateurs apotec®. WEPA informera l'utilisateur par écrit de toute augmentation de la rémunération en temps utile, au plus tard 3 mois avant son entrée en vigueur. Une augmentation de prix ne doit pas dépasser de plus de 10 % la rémunération actuelle.

En cas d'augmentation de prix, l'utilisateur est en droit de résilier le contrat par écrit dans un délai de trois mois à compter de la réception de l'annonce visée à la deuxième phrase. WEPA attire expressément l'attention sur cette possibilité de résiliation dans l'avis visé à la 2ephrase. Si aucune résiliation n'intervient dans ce délai, la nouvelle redevance d'utilisation communiquée par WEPA s'applique.

**7. Modifications du système**

7.1 Dans le cadre du développement de ses produits, WEPA est autorisée à modifier les systèmes de surveillance des réfrigérateurs apotec®, notamment pour les adapter aux conditions juridiques, légales, économiques et techniques.

**8. Responsabilité**

8.1 Les demandes de dommages et intérêts de l'utilisateur pour des dommages de quelque nature que ce soit sont exclues. La limitation de responsabilité s'applique également aux représentants légaux et aux auxiliaires d'exécution de WEPA, dans la mesure où l'utilisateur fait valoir des droits à leur encontre.

8.2 Sont exclues de la limitation de responsabilité susmentionnée les demandes de dommages et intérêts résultant d'un manquement intentionnel ou par négligence grave aux obligations de WEPA, d'un représentant légal ou d'un auxiliaire d'exécution. Est également exclue de cette limitation de responsabilité la violation, au moins par légère négligence, d'obligations contractuelles essentielles. Les obligations contractuelles essentielles sont celles dont l'exécution permet l'exécution en bonne et due forme du contrat et sur l'exécution desquelles l'utilisateur peut compter.

8.3 La limitation de responsabilité susmentionnée n'affecte pas la responsabilité indépendante de la faute prescrite par la loi, en particulier la responsabilité selon la loi sur la responsabilité du fait des produits, ni la responsabilité en cas d'atteinte fautive à la vie, à l'intégrité physique ou à la santé d'un utilisateur.

**9. Disponibilité**

9.1 Il n'existe aucun droit à une utilisation ininterrompue. Il n'est pas garanti que l'accès ou l'utilisation de la surveillance des réfrigérateurs apotec® ne soit pas interrompu ou affecté par des travaux de maintenance, des développements ou d'autres perturbations. WEPA s'efforce d'assurer une utilisation aussi ininterrompue que possible d'apotec® Surveillance des réfrigérateurs et informera l'utilisateur à l'avance des travaux de maintenance prévus. Toutefois, des restrictions ou des interruptions temporaires peuvent survenir en raison de perturbations techniques (telles que l'interruption de l'alimentation électrique, des pannes de matériel et de logiciel, des problèmes techniques dans les lignes de données).

**10. Protection des données**

10.1 Les parties s'engagent à traiter les données à caractère personnel dans le respect des dispositions légales applicables en matière de protection des données.

10.2 Dans la mesure où WEPA traite des données personnelles des em-ployés de l'utilisateur dans le cadre de la fourniture des prestations, les parties conviennent de traiter ces données personnelles conformément à l'article 28 du RGPD dans le cadre de l'accord de traitement des commandes joint dans l'annexe1

**11. Droits d'auteur, droits de marquage et autres droits de propriété intellectuelle**

11.1 Les contenus disponibles dans la surveillance des réfrigérateurs apotec® (textes, données, images, logos, graphiques, documentations, représentations sonores, vidéo et autres images) sont soumis au droit d'auteur et à d'autres lois sur la protection de la propriété intellectuelle. Il est interdit de reproduire, de diffuser, d'enregistrer ou de modifier tout ou partie des contenus dans d'autres médias (par exemple d'autres sites Internet) sans l'accord préalable exprès du titulaire des droits.

**12. Modifications des conditions d'utilisation**

12.1 WEPA se réserve le droit de modifier certaines clauses des présentes conditions d'utilisation avec effet pour l'avenir et sans indication de motifs, dans la mesure où cela est acceptable pour l'utilisateur et compte tenu des intérêts de WEPA. WEPA informera l'utilisateur en temps utile de toute modification des conditions d'utilisation. Si l'utilisateur ne s'oppose pas à la modification des conditions d'utilisation dans un délai de six semaines après l'entrée en vigueur des conditions d'utilisation modifiées, les conditions d'utilisation modifiées sont considérées comme acceptées. Si l'utilisateur s'oppose aux modifications, WEPA est en droit de résilier le contrat d'utilisation, dans le cas où le maintien de la relation contractuelle dans le cadre des conditions d'utilisation actuelles n'est pas possible ou raisonnable en tenant compte des intérêts de l'utilisateur.

**13. Dispositions finales**

13.1 Le droit de la République fédérale d'Allemagne s'applique exclusivement aux présentes conditions d'utilisation et à leur interprétation. L'application du droit privé international allemand ou européen ainsi que de la Convention des Nations Unies sur les contrats de vente internationale de marchandises est exclue.

13.2 Le tribunal compétent exclusif et le lieu d'exécution pour les litiges découlant de ces conditions d'utilisation ou en rapport avec celles-ci est le siège de WEPA.

13.3 Si certaines dispositions des présentes conditions d'utilisation sont ou deviennent nulles et/ou inapplicables, la validité des autres dispositions n'en est pas affectée. Les dispositions nulles et/ou inapplicables seront remplacées, par voie d'interprétation complémentaire du contrat, par les dispositions valides et applicables qui, compte tenu des intérêts des deux parties, sont les plus appropriées pour atteindre l'objectif économique souhaité. Il en va de même pour combler les lacunes des présentes conditions d'utilisation.

Version : 04/2024

## Annexe 1 : Accord sur le traitement des commandes selon l'art. 28 du RGPD

Dans la mesure où WEPA (ci-après dénommée « sous-traitant » dans la présente annexe) traite les données personnelles des employés de l'utilisateur (ci-après dénommé : « responsable ») dans le cadre de la fourniture de prestations, les accords de traitement des commandes définis ci-après s'appliquent.

**1. Objectif et champ d'application**

1.1 Le présent contrat de traitement des données à caractère personnel (ci-après les « clauses ») est essentiellement basé sur les clauses contractuelles types figurant en annexe de la DÉCISION D'EXÉCUTION (UE) 2021/915 DE LA COMMISSION du 4 juin 2021 relative aux clauses contractuelles types entre responsables et sous-traitants en application de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil.

1.2 Ces clauses visent à garantir le respect de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 qui est relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et qui abroge la directive 95/46/CE (règle-ment général sur la protection des données).

1.3 Les parties ont accepté ces clauses afin de garantir le respect de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679.

1.4 Les présentes clauses s'appliquent au traitement des données à caractère personnel conformément à l'annexe I.

1.5 Les annexes I à III font partie intégrante des clauses.

1.6 Les présentes clauses s'appliquent sans préjudice des obligations auxquelles le responsable est soumis en vertu du règlement (UE) 2016/679.

1.7 Les présentes clauses ne garantissent pas, à elles seules, le respect des obligations relatives aux transferts internationaux de données prévues au chapitre V du règlement (UE) 2016/679.

**2. Interprétation**

2.1 Lorsque les termes définis dans le règlement (UE) 2016/679 sont utilisés dans les présentes clauses, ces termes ont la même signification que dans le règlement concerné.

2.2 Ces clauses doivent être interprétées à la lumière des dispositions du règlement (UE) 2016/679.

2.3 Ces clauses ne doivent pas être interprétées d'une manière qui irait à l'encontre des droits et obligations prévus par le règlement (UE) 2016/679 ou qui porterait atteinte aux libertés et droits fondamentaux des personnes concernées.

**3. Description du traitement**

Les détails des opérations de traitement, notamment les catégories de données à caractère personnel et les finalités pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable sont indiqués à l'annexe I.

**4. Obligations des parties**

**4.1 Instructions**

4.1.1 Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable, à moins qu'il ne soit tenu de le faire en vertu du droit de l'Union européenne ou du droit d'un État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable de ces exigences légales avant le traitement, à moins que le droit concerné ne l'interdise pour un motif d'intérêt public important. Le responsable peut donner des instructions supplémentaires pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

4.1.2 Le sous-traitant informe le responsable s'il estime que les instructions données par le responsable sont contraires au règlement (UE) 2016/679 ou à la législation de l'Union ou des États membres en vigueur en matière de protection des données.

**4.2 Limitation des finalités**

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques mentionnées à l'annexe I, à condition qu'il ne reçoive pas d'autres instructions du responsable.

**4.3 Durée du traitement des données à caractère personnel**

Les données à caractère personnel ne sont traitées par le sous-traitant que pour la durée indiquée à l'annexe I.

**4.4 Sécurité du traitement**

4.4.1 Le sous-traitant met en œuvre au moins les mesures techniques et organisationnelles énumérées à l'annexe II afin de garantir la sécurité des données à caractère personnel. Cela inclut la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès non autorisé à celles-ci (ci-après dénommée « violation de données à caractère personnel »). Pour évaluer le niveau de protection adéquat, les parties tiennent dûment compte de l'état de actuel des techniques en la matière, des coûts d'implémentation, de la nature, de la portée, des circonstances et des finalités du traitement, ainsi que des risques encourus par les personnes concernées..

4.4.2 Le sous-traitant n'accorde à son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure où cela est nécessaire pour l'exécution, la gestion et le suivi du contrat. Le sous-traitant veille à ce que le personnel autorisé à traiter les données à caractère personnel reçues s'engage à respecter la confidentialité ou soit soumis à une obligation légale de secret professionnel appropriée.

**4.6 Documentation et respect des clauses**

4.6.1 Les parties doivent être en mesure de prouver le respect des présentes clauses.

4.6.2 Le sous-traitant répondra rapidement et de manière appropriée aux demandes du responsable concernant le traitement des données conformément aux présentes clauses.

4.6.3 Le sous-traitant met à la disposition du responsable toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679. À la demande du responsable, le sous-traitant autorise également et contribue à l'audit des activités de traitement couvertes par les présentes clauses à des intervalles appropriés ou en cas d'indices de non-respect. Lorsqu'il décide d'un examen ou d'un audit, le responsable peut tenir compte des certifications pertinentes du sous-traitant et/ou de ses sous-traitants.

4.6.4 Le responsable peut effectuer l'audit lui-même ou faire appel à un auditeur indépendant. Les audits peuvent également inclure des inspections dans les locaux ou les installations physiques du sous-traitant. Pour effectuer les inspections, le responsable est autorisé à pénétrer dans les locaux du sous-traitant où des données à caractère personnel sont traitées pour le compte du responsable, dans le cadre des heures de bureau habituelles, après un préavis raisonnable (en règle générale, au moins 14 jours civils), à moins que, dans un cas particulier, une inspection sans préavis ne paraisse absolument nécessaire pour l'ob-jectif du contrôle, et ce à ses propres frais,

sans perturber outre mesure le fonctionnement de l'entreprise et en respectant strictement la confidentialité des secrets industriels et commerciaux du Sous-traitant. Les inspections sont en principe limitées à une fois par année civile. Il n'est pas dérogé à cette règle pour les inspections effectuées pour des raisons importantes que le responsable doit exposer. Le sous-traitant prend en charge les coûts de l'inspection dans la mesure où celle-ci a été rendue nécessaire par une violation de la loi ou du contrat par le sous-traitant.

4.6.5 Si le responsable charge un auditeur indépendant d'effectuer le contrôle, le responsable doit engager par écrit l'auditeur indépendant de la même manière que le responsable est engagé envers le sous-traitant sur la base de la présente clause (4.6). En outre, le responsable doit obliger l'auditeur indépendant à respecter la confidentialité et le secret professionnel, à moins que l'auditeur indépendant ne soit soumis à une obligation de confidentialité professionnelle. Sur la demande du sous-traitant, le responsable doit lui fournir sans délai les accords d'engagement conclus avec l'auditeur indépendant Le responsable ne doit pas confier l'inspection à un concurrent du sous-traitant.

4.6.6 Le sous-traitant est autorisé, à sa seule discrétion et dans le respect des obligations légales du responsable, à ne pas divulguer des informations qui sont sensibles par rapport à ses activités de sous-traitant ou si la divulgation de telles informations par le sous-traitant constitue une violation de la loi ou d'autres dispositions contractuelles. Le responsable n'est pas autorisé à accéder aux données ou aux informations concernant d'autres clients du sous-traitant, aux informations relatives aux coûts, aux rapports d'audit de qualité et de gestion des contrats, ainsi qu'à toutes les autres données confidentielles du sous-traitant qui ne sont pas directement pertinentes pour les objectifs de contrôle convenus.

**4.7 Recours à des sous-traitants secondaires**

4.7.1 Le sous-traitant dispose de l'autorisation générale du responsable pour faire appel aux sous-traitants mentionnés dans la liste convenue figurant à l'annexe III. Le sous-traitant informe expressément le responsable, par écrit et au moins 14 jours calendaires à l'avance, de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants, et donne ainsi au responsable suffisamment de temps pour s'opposer à ces modifications avant d'engager le ou les sous-traitants concernés. Le sous-traitant fournit au responsable les informations nécessaires pour que celui-ci puisse exercer son droit d'opposition.

4.7.2 Si le sous-traitant charge un sous-traitant ultérieur d'effectuer certaines activités de traitement (pour le compte du responsable), cette charge doit être effectuée par le biais d'un contrat qui impose au sous-traitant ultérieur des obligations en matière de protection des données substantiellement identiques à celles qui s'appliquent au sous-traitant conformément aux présentes clauses.

**4.8 Transferts internationaux de données**

Le responsable accepte que, dans les cas où le sous-traitant fait appel à un sous-traitant ultérieur conformément à la clause 4.7 pour l'exécution de certaines activités de traitement (pour le compte du responsable) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du Règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent assurer le respect du chapitre V du Règlement (UE) 2016/679 en utilisant un mécanisme de sauvegarde conformément aux articles 44 et suivants du Règlement (UE) 2016/679. RGPD (notamment une décision d'adéquation ou des clauses contractuelles types adoptées par la Commission conformément à l'article 46, paragraphe 2, du règlement (UE) 2016/679).

**5. Assistance au responsable**

5.1 Le sous-traitant informe sans délai le responsable de toute demande qu'il a reçue de la personne concernée. Il ne répond pas lui-même à la demande, sauf s'il a été autorisé à le faire par le responsable.

5.2 Compte tenu de la nature du traitement, le sous-traitant aide le res-ponsable à remplir son obligation de répondre aux demandes d'exercice des droits des personnes concernées.

5.3 Outre l'obligation du sous-traitant d'aider le responsable conformément à la clause 5.2, le sous-traitant, compte tenu de la nature du traitement des données et des informations dont il dispose, aide également le responsable à respecter les obligations visées aux articles 32 à 36.

**6. Notification des violations de la protection des données à caractère personnel**

En cas de violation de la protection des données à caractère personnel, le sous-traitant coopère avec le responsable et lui apporte une assistance appropriée afin de permettre au responsable de s'acquitter de ses obligations au titre des articles 33 et 34 du règlement (UE) 2016/679, en tenant compte de la nature du traitement et des informa-tions dont il dispose.

**7. Violation des clauses et résiliation du contrat**

7.1 Si le sous-traitant ne respecte pas ses obligations au titre des présentes clauses, le responsable peut, sans préjudice des dispositions du règlement(UE) 2016/679, ordonner au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce qu'il se conforme aux présentes clauses ou jusqu'à la résiliation du contrat. Le sous-traitant informe immédiatement le responsable si, pour quelque raison que ce soit, il n'est pas en mesure de respecter ces clauses.

7.2 Le sous-traitant est en droit de résilier le contrat dans la mesure où les instructions données par le responsable sont contraires au règlement (UE) 2016/679 ou à la législation de l'Union ou des États membres en vigueur en matière de protection des données et que le responsable du traitement insiste sur l'exécution de ces instructions après avoir été informé par le sous-traitant que ses instructions sont contraires aux exigences légales applicables conformément à la clause 4.1.2.

7.4 Après la résiliation du contrat, le sous-traitant, au choix du responsable, efface toutes les données à caractère personnel traitées pour le compte du responsable et certifie au responsable que cela a été fait, ou restitue au responsable toutes les données à caractère personnel et efface les copies existantes, sauf si le droit de l'Union ou le droit des États membres impose de conserver les données à caractère personnel. Jusqu'à l'effacement ou la restitution des données, le sous-traitant continue à garantir le respect de ces clauses.

## ANNEXE I - Description du traitement

**Catégories de personnes concernées dont les données à caractère personnel sont traitées**

- Employés du responsable

**Catégories de données à caractère personnel traitées**

- Fichiers journaux, tels que l'adresse IP, l'identifiant unique de l'utilisateur (UPN), la date et l'heure de la consultation et le type de consultation, le type et la version du navigateur utilisé, le système d'exploitation utilisé, l'URL de la page du portail au moment de la consultation, les actions effectuées sur le portail, les consultations de services de base
- Données d'authentification, telles que l'identifiant unique (UPN), l'adresse de l'entreprise, l'identifiant de la société, le prénom et le nom, l'adresse e-mail, le numéro de téléphone
- Données relatives aux appareils de réfrigération et de congélation et au SmartModul, telles que le modèle, le numéro de série, le numéro d'article et les données télémétriques telles que la température, l'état d'ouverture de la porte, les données de réseau (telles que l'adresse Mac et IP du SmartModul, l'état du réseau (W)LAN)
- Fonctions de notification par e-mail (identifiant unique de l'utilisateur (UPN), identifiant de la société, adresse e-mail du destinataire, métadonnées des messages, contenu du message, adresse de la société, liens vers des rapports).
- Fonction de notification par SMS et appel téléphonique (identifiant unique (UPN), identifiant de la société, numéro de téléphone du destinataire, métadonnées des messages, contenu du message ou de la notification d'appel)

Données sensibles traitées (le cas échéant) et restrictions ou garanties appliquées tenant pleinement compte de la nature des données et des risques associés, telles qu'une limitation stricte des finalités, des restrictions d'accès (y compris l'accès réservé aux employés ayant suivi une formation spécifique), des enregistrements de l'accès aux données, des restrictions sur les transferts ultérieurs ou des mesures de sécurité supplémentaires.

- Aucune donnée sensible n'est traitée.

**Type du traitement**

- Le type du traitement est décrit concrètement dans les conditions d'utilisation. L'application basée sur un navigateur permet d'enregistrer en continu les températures, les états d'alarme et les états de commutation des composants. Il est possible de paramétrer une alarme en cas de température trop élevée ou trop basse. L'alarme peut être envoyée par e-mail ou par SMS. En outre, des rapports peuvent être créés et téléchargés afin de pouvoir satisfaire, le cas échéant, à diverses obligations de documentation

**Finalité(s) pour laquelle/lesquelles les données à caractère personnel sont traitées pour le compte du responsable**

- Garantie de la stabilité et de la sécurité du réseau et de l'information
- Authentification sur le portail dans le cadre de l'utilisation
- Gestion des utilisateurs et des autorisations sur le portail
- Envoi de notifications
- Transmission de rapports par voie numérique
- Dernière langue choisie pour le portail, internationalisation du login
- Enregistrement des données de connexion après une connexion réussie (comme le nom, l'UPN, les jetons)

**Durée du traitement**

- La durée du traitement correspond à la durée de l'accord d'utilisation.

## ANNEXE II - Mesures techniques et organisationnelles y compris pour assurer la sécurité des données

Pour la mise à disposition et l'hébergement du portail, le sous-traitant a re-cours aux services de sous-traitants dont les mesures techniques et organisationnelles sont présentées ci-dessous:

### 1. Confidentialité

### 1.1 Contrôle d'accès

Objectif : Pas d'accès non autorisé aux installations de traitement des données

- Système de contrôle d'accès automatique, lecteur de badge
- Cartes à puce / systèmes de transpondeur
- Système de fermeture à deux facteurs dans le Data Center (bio-métrie)
- Réglementations d'accès pour pénétrer dans le Data Center
- Système de fermeture manuel
- Serrures de sécurité
- Régulation des clés / liste / documentation
- Sécurisation des portes
- Portes avec bouton côté extérieur
- Portes électroniques
- Entrées principales fermées en dehors des heures de bureau
- Accès possible uniquement avec un badge
- Accès des visiteurs uniquement par la réception
- Protocole des visiteurs
- Clôture de l'usine
- Barrières/dispositifs de séparation
- Badges pour les employés et les visiteurs
- Visiteurs accompagnés par des collaborateurs
- prise en charge personnelle des visiteurs
- Sécurisation du site par des gardiens
- Sécurisation par des caméras
- Soin apporté à la sélection du personnel de sécurité

### 1.2 Contrôle d'accès

Objectif : pas d'utilisation non autorisée du système

- Login avec nom d'utilisateur + mot de passe
- Politique de mot de passe
- Politique générale de sécurité informatique (politique d'utilisation de l'ordinateur, politique de mot de passe, politique de compte, appareil mobile, etc.)
- Verrouillage automatique du bureau
- Logiciel antivirus de nouvelle génération Clients
- Logiciel antivirus de nouvelle génération Serveur
- Protection du BIOS (avec PIN/mot de passe)
- Verrouillage des interfaces externes
- Cryptage des ordinateurs portables / tablettes
- Cryptage de supports de données
- Gestion des droits d'accès des utilisateurs

- Système de gestion des accès aux identités
- Chiffrement des smartphones
- Gestion des appareils mobiles
- Contrôle d'accès au réseau LAN/WIFI (NAC)
- Pare-feu
- Utilisation de la technologie VPN
- Création de rôles d'utilisateurs
- Système de gestion des mots de passe

### 1.3 Contrôle d'accès

Objectif : pas de lecture, de copie, de modification ou de suppression non autorisées à l'intérieur du système.

- Utilisation de concepts d'autorisation
- Gestion des autorisations par les administrateurs
- Autorisation des autorisations par les propriétaires des données
- Nombre minimal d'administrateurs système/d'administrateurs d'applications
- Utilisation sécurisée des interfaces USB
- Stockage sécurisé des supports de données
- Coffre-fort pour les sauvegardes
- Destruction appropriée des supports de données
- Destructeur de documents externe ou prestataire de services selon les directives actuelles sur les données.
- Déchiqueteuse de dossiers
- Consignation des accès aux applications / serveurs

### 1.4 Contrôle de la séparation

Objectif : traitement séparé des données collectées à des fins différentes.

- Séparation de l'environnement de production et de l'environnement de test
- Séparation physique (systèmes / bases de données / supports de données)
- Contrôle par le biais du concept d'autorisation
- Contrôle régulier des autorisations
- Séparation des données et des systèmes / applications
- Colocation des applications pertinentes
- Définition des droits d'accès aux bases de données

### 1.5 Pseudonymisation

Objectif : traitement de données à caractère personnel de telle sorte que les données ne puissent plus être attribuées à une personne concernée sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles appropriées ;

- Transmission des données sous forme anonymisée, pseudonymisée ou cryptée
- Instructions internes sur le traitement soigneux des données personnelles
- Suppression des données à caractère personnel à l'expiration du délai légal de suppression.
- Séparation des données d'attribution

## 2. Intégrité

### 2.1 Contrôle de la transmission

Objectif : pas de lecture, de copie, de modification ou de suppression non autorisée lors de la transmission ou du transport électronique

- Cryptage des e-mails lors du transport (au sein du groupe)
- Utilisation de connexions dédiées
- Utilisation de VPN
- Asset des supports de données et attribution aux personnes
- Enregistrement des accès et des consultations
- Conteneurs de transport sécurisés
- Mise à disposition via des connexions cryptées
- Rigueur dans le choix du personnel de transport et des véhicules
- Remise en main propre avec protocole et signature
- Utilisation de signatures
- Utilisation de certificats

### 2.2 Contrôle de l'entrée

Objectif : déterminer si des données à caractère personnel ont été introduites, modifiées ou supprimées dans les systèmes de traitement des données et, le cas échéant, par qui

- Enregistrement technique de l'introduction, de la modification et de la suppression des données
- Contrôles de plausibilité réguliers
- Délais de conservation et de suppression
- Responsabilités claires en matière d'effacement
- Traçabilité des saisies, modifications et suppressions de don-nées par des noms d'utilisateurs individuels
- Attribution de droits pour la saisie, la modification et la suppression de données sur la base d'un concept d'autorisation avec le propriétaire des données et les autorisations
- Enregistrement des modifications qui sont reprises dans les traitements automatiques

## 3. Disponibilité et résistance

Objectif : protection contre la destruction ou la perte accidentelle ou intentionnelle.

- Systèmes de serveurs et de stockage dans le Data Center sécurisé
- Data center climatisé
- Systèmes de détection d'incendie et de fumée, ainsi que de détection précoce d'incendie
- Surveillance de la température et de l'humidité du Data Center
- Surveillance par caméra dans le Data Center
- Messages lors de l'accès au Data Center
- Pas de raccordements sanitaires dans le Data Center
- Extincteurs dans et / ou devant le Data Center
- Installations UPS redondantes
- Protection contre les influences environnementales (tempête, eau)
- Système RAID / mise en miroir des disques durs
- Partitions séparées pour les systèmes d'exploitation et les données
- Mises à jour régulières des logiciels
- Réalisation régulière d'une analyse des points faibles du matériel et des logiciels

- Système de protection contre les virus
- Concept de sauvegarde et de récupération
- Contrôle du processus de sauvegarde
- Tests réguliers de récupération des données et journalisation des résultats
- Existence d'un plan d'urgence
- Conservation des supports de sauvegarde dans un endroit sûr en dehors du Data Center.
- Coffre-fort de protection des données

**4. Procédures de contrôle, d'évaluation et de suivi réguliers.**

**Gestion de la protection des données**

- Délégué interne à la protection des données
- Organisation de la protection des données/gestion de la protection des données
- Guides de protection des données/recommandations d'action
- Documentation centrale de toutes les activités de traitement et des règles relatives à la protection des données avec possibilité d'accès pour les collaborateurs en fonction des besoins / autorisations
- Processus formalisé pour le traitement des demandes d'information de la part des personnes concernées est disponible
- L'évaluation de l'impact sur la protection des données (DSFA) est effectuée si nécessaire.
- Les collaborateurs sont formés ou sensibilisés à la protection des données
- Les collaborateurs sont tenus à la confidentialité/au secret des données

**Gestion de la sécurité informatique**

- Responsable interne de la sécurité de l'information
- Système de gestion de la sécurité de l'information
- Politique de sécurité informatique de Liebherr
- Audits réguliers de la sécurité informatique
- Formation des employés sur la sécurité des données

**Réponse aux incidents**

- Système de prévention des intrusions (IPS)
- 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
- Procédure documentée de gestion des incidents de sécurité
- Documentation des incidents de sécurité et des violations de données
- Implication du DPD et de l'USIC dans les incidents de sécurité et les pannes de données
- Processus formel et responsabilités pour le suivi des incidents de sécurité et des violations de données
- Processus documenté de détection et de notification des incidents de sécurité/violations de données (également en ce qui concerne l'obligation de notification à l'autorité de surveillance)

**Paramètres par défaut favorables à la protection des données**

- Le nombre de données personnelles collectées ne dépasse pas ce qui est nécessaire pour chaque objectif.
- Exercice simple du droit de rétractation de la personne concernée grâce à des mesures techniques.

**Contrôle des mandats**

- Modèles d'accords existants pour le traitement des commandes
- Processus défini pour une rédaction claire du contrat
- Sélection rigoureuse des sous-traitants
- Examen des accords
- Contrôle de l'exécution du contrat

## ANNEXE III - Liste des sous-traitants secondaires

Le responsable a autorisé le recours aux sous-traitants suivants

| Nom | Adresse | Personne de contact | Description du Traitement |
|---|---|---|---|
| Liebherr-Hausgeräte Vertriebs- und Service GmbH | Konrad-Zuse-Straße 4+6, 89081 Ulm, Deutschland | | Mise à disposition et hébergement du portail |
| Liebherr-Hausgeräte Ochsenhausen GmbH (en tant que sous-traitant de Liebherr-Hausgeräte Vertriebs- und Ser-vice GmbH) | Memminger Straße 77 79, 88416 Ochsen-hausen, Allemagne | | Hébergement Azure Cloud, mise à disposition & assistance technique du portail, authentification, gestion des licences |



WEPA Apothekenbedarf GmbH & Co KG, D-56204 Hillscheid
www.wepa-apothekenbedarf.de
T +49 (0)2624 107-361
F +49 (0)800 5252500 (gebührenfrei)
info@wepa-apothekenbedarf.de
wepa.shop
wepa.cloud
wepa.school