Accord sur le traitement des ordres de commandes
pour

Produits numériques Jungheinrich

(ci-après : « **Accord** »)

entre le **client** et **Jungheinrich**

- le client et Jungheinrich sont également dénommés « **partie** » et ensemble les « **parties** » ci-après -

PREAMBULE

A. Les parties ont conclu un contrat pour la mise à disposition de produits numériques Jungheinrich sur la base de la page de garde du contrat et des conditions générales d'utilisation des produits numériques Jungheinrich d'avril 2023 (« CGU ») (la page de garde du contrat et les CGU constituent ensemble le « contrat principal »). Dans le cadre de la mise à disposition des produits numériques Jungheinrich, Jungheinrich traite, pour le compte du client, des données à caractère personnel dans la mesure décrite dans l'annexe 2 et l'annexe 4 du présent contrat. Le présent accord fait partie intégrante du contrat principal et constitue une annexe de celui-ci.

B. Les parties conviennent que les dispositions suivantes s'appliquent au traitement des données personnelles par Jungheinrich sur ordre du client dans le cadre de l'exécution des prestations contractuelles.

1. **DEFINITIONS**

Aux fins du présent accord, les parties définissent les termes suivants et découlant du règlement général européen relatif à la protection des données. Les parties entendent la notion fondamentale que d'autres actes législatifs applicables en matière de protection des données, tels que la loi suisse sur la protection des données, utilisent certes parfois d'autres termes, mais que leur signification correspond pour l'essentiel à celle des termes du RGPD (p. ex. « données à caractère personnel » [RGPD] et « données personnelles » [LPD]).

Dans le cadre du présent accord, les termes suivants ont la signification qui leur est respectivement attribuée comme suit :

1.1 « **Droit applicable à la protection des données** » désigne les lois, prescriptions et réglementations mentionnées au point 2.3.

1.2 « **Responsable du traitement de l'ordre de commande** » désigne une personne privée physique ou morale, une autorité, une institution ou un autre organisme qui traite des données personnelles sur ordre du responsable. Jungheinrich est responsable du traitement de l'ordre de commande dans le cadre du traitement des données personnelles qu'il effectue sur ordre du client dans l'étendue prévue par le présent accord.

1.3 « **Personne concernée** » désigne la personne physique que concernent les données personnelles traitées.

1.4 « **LPD** » désigne la Loi fédérale suisse sur la protection des données du 25 septembre 2020 (en vigueur au 1er septembre 2023).

1.5 « **RGPD** » désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles, à la libre circulation des données et à la suppression de la directive 95/46/CE (règlement général sur la protection des données).

1.6 « **Entreprise associée impliquée** » désigne une entreprise associée (i) au nom et sur ordre de laquelle la partie qui est associée à l'entreprise a conclu le présent accord (point 3.1), ou (ii) qui a adhéré ultérieurement au présent accord conformément au point 3.2.

1.7 Les « **données personnelles** » sont toutes les informations se rapportant à une personne physique identifiée ou identifiable.

1.8 « **Sous-traitant(s)** » désigne un autre ou d'autres responsables du traitement de l'ordre de commande au sens de l'article 9 de la LPD (article 28, paragraphes 2 et 4 du RGPD).

1.9 « **Responsable** » désigne la personne privée physique ou morale, l'autorité, l'institution ou tout autre organisme qui, seul(e) ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles. Le client est responsable du traitement des données personnelles par Jungheinrich sur ordre du client dans l'étendue prévue par le présent accord.

1.10 « **Traitement** » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés en relation avec des données personnelles telles que la collecte, la saisie, l'organisation, le classement, la sauvegarde, l'adaptation ou la modification, la lecture, la recherche, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, la comparaison ou la liaison, la limitation, la suppression ou la destruction.

1.11 « **Entreprise associée** » au sens du présent accord désigne toute autre entreprise relative à l'une des parties qui, directement ou indirectement, contrôle, est contrôlée par ou se trouve sous contrôle commun avec la partie concernée. « Contrôle » au sens de la présente définition signifie la propriété directe ou indirecte ou la possession de plus de cinquante pour cent (50 %) des droits de vote d'une entreprise ; les termes « contrôlant », « contrôlé par » ou « sous contrôle commun » ont les significations correspondantes à ce qui précède.

2. OBJET ET DUREE DE L'ACCORD ; DROIT APPLICABLE

2.1 Objet de l'accord

Le présent accord a pour objet le traitement des données personnelles par Jungheinrich (en tant que responsable du traitement de l'ordre de commande) sur ordre du client (en tant que responsable) conformément aux dispositions du contrat principal, au présent traitement des ordres de commandes et aux directives et instructions du client. Les processus de traitement des données sous la propre responsabilité de Jungheinrich ne sont pas affectés par le présent accord. Voir également le point 4.5 à ce sujet.

2.2 Durée de l'accord ; résiliation

Le présent accord entre en vigueur à la signature du contrat principal, mais au plus tard lorsque Jungheinrich accède pour la première fois aux données personnelles du client. La durée du présent accord correspond à la durée du contrat principal.

Les réglementations concernant la résiliation du contrat principal et le point 11.3 du présent accord sont valables.

2.3 Droit applicable en matière de protection des données et juridiction compétente

Sont déterminantes pour le traitement des données du responsable par le responsable et/ou le responsable du traitement de l'ordre de commande :

(1) les dispositions de la LPD suisse et les ordonnances y afférentes ;

et le cas échéant :

(2) les dispositions du RGPD et les réglementations nationales pertinentes des États membres de l'Union européenne relatives à la mise en œuvre et à l'introduction du RGPD ;

(3) les lois et réglementations nationales en matière de protection des données des États parties à l'accord sur l'Espace économique européen (EEE) ;

(4) les autres lois et dispositions relatives à la protection des données en vigueur au siège des parties.

Par ailleurs, le contrat principal détermine le droit applicable à la présente convention et le for juridique.

3. PARTIES DE L'ACCORD

3.1 Inclusion d'entreprises associées

Chaque partie conclut le présent accord en son nom propre ainsi qu'au nom et pour le compte de ses entreprises affiliées, dans la mesure où une procuration correspondante a été établie. Toute entreprise associée du client ainsi impliquée sera tenue de respecter les dispositions du présent accord et, le cas échéant, du contrat principal, et aura les droits et obligations d'un responsable découlant du présent accord. Les entreprises associées impliquées ne deviennent pas parties du contrat principal par cette réglementation, mais seulement parties du présent accord. Les parties sont tenues de documenter l'existence d'une procuration en bonne et due forme et de la prouver sous une forme appropriée à la demande de l'autre partie. Afin de documenter les entreprises associées qui sont parties du présent accord, les parties échangeront et mettront à jour, si nécessaire, une liste des entreprises associées impliquées.

3.2 Adhésion ultérieure

Une entreprise associée du client n'étant pas partie du présent accord au moment de la conclusion du contrat peut y adhérer à tout moment en signant et en transmettant à Jungheinrich une déclaration d'adhésion conforme au modèle figurant dans l'**Annexe 1** . Dans le cas où Jungheinrich ne s'oppose pas à l'adhésion dans un délai de deux (2) semaines par notification écrite, l'entreprise associée adhérente devient partie du présent accord et a dès lors les droits et obligations d'un responsable découlant du présent accord. Aucun droit ou obligation découlant du présent accord ne s'applique à l'entreprise associée adhérente pour la période précédant son adhésion en tant que partie.

Dans le cas où, du côté de Jungheinrich, une entreprise associée doit reprendre l'activité de traitement dans son intégralité ou dans un pays contractuel, la réglementation mentionnée ci-dessus s'applique par analogie, à condition que l'entreprise associée de Jungheinrich qui adhère informe le client ou la ou les entreprise(s) associée(s) impliquée(s) du client pour laquelle ou lesquelles elle reprendra les activités de traitement par une notification correspondante (au lieu d'utiliser le modèle de déclaration d'adhésion).

3.3 Communication

Le client qui est partie du contrat principal coordonne la communication de ses entreprises associées impliquées avec Jungheinrich au titre du présent accord et est seul responsable de la communication avec Jungheinrich au titre du présent accord. Jungheinrich peut exiger que la communication avec Jungheinrich soit effectuée exclusivement par le client, et non par les entreprises associées impliquées.

3.4 Exercice collectif des droits

Sauf si l'exercice d'un droit ou d'un recours découlant du présent accord par l'entreprise associée impliquée du côté du client lui-même est prescrit par la loi, l'exercice des droits découlant du présent accord qui reviennent aux entreprises associées impliquées du côté du client en vertu du droit applicable en matière de protection des données ne peut être effectué

i. que par le client, qui est partie du contrat principal, pour les entreprises associées impliquées du côté du client, et

ii. uniquement de manière collective, c'est-à-dire non pas individuellement pour chaque entreprise associée impliquée, mais collectivement pour lui-même et toutes les entreprises associées impliquées.

Cet exercice collectif des droits se rapporte également à l'exercice des droits de contrôle selon le point 12. Dans ce contexte, le client, qui est partie du contrat principal, veillera à ce que la perturbation de l'exploitation de Jungheinrich lors d'éventuels contrôles sur place soit aussi limitée que possible, en regroupant, dans la mesure du possible, les demandes de contrôle de plusieurs entreprises associées impliquées pour un contrôle sur place.

4. CONCRETISATION DU CONTENU DE L'ACCORD

4.1 Étendue, type et but du traitement des données sur ordre.

Les données à caractère personnel sont traitées par Jungheinrich sur ordre du client dans la mesure nécessaire à la fourniture des prestations convenues en vertu du contrat principal. L'étendue dépend donc des produits numériques et des solutions logicielles de Jungheinrich auxquels se rapportent les prestations de Jungheinrich. Les détails concernant le traitement des données par Jungheinrich sur ordre du client, en particulier les catégories de données à caractère personnel, les catégories de personnes concernées, les finalités du traitement des données à caractère personnel sur ordre du client et la durée de conservation régulière sont décrits dans l'**Annexe 2**, **Annexe 3** et l'**Annexe 4**.

4.2 Lieu du traitement des données | Transmission de données à l'étranger

Le traitement contractuel des données a fondamentalement lieu en Suisse, dans un état membre de l'Union européenne (UE) ou dans un autre état faisant partie de l'accord dans l'Espace Économique Européen (EEE).

Toute transmission de données par Jungheinrich vers un pays situé en dehors de l'UE ou de l'EEE (« **pays tiers** ») se fait uniquement sur la base d'instructions documentées du client et doit être conforme au droit applicable en matière de protection des données, conformément au [point 2.3] (art. 16-18 LPD ; si applicable le chapitre V du RGPD, entre autres).

Le client accepte que, dans les cas où Jungheinrich charge un sous-traitant, conformément au point 11, d'exécuter certaines activités de traitement (sur ordre du client) et où l'activité de traitement implique une transmission de données personnelles vers un pays tiers au

sens du chapitre V du RGPD, le traitement des données puisse avoir lieu dans un pays tiers en dehors de la Suisse / de l'UE / de l'EEE si

- il existe une décision du Conseil fédéral (et, en cas d'application du RGPD, de la Commission européenne) selon laquelle un niveau de protection adéquat est assuré dans ce pays tiers, ou si
- Jungheinrich et le sous-traitant utilisent des clauses contractuelles standard qui ont été préalablement approuvées, émises ou reconnues par le Conseil fédéral (ou, si le RGPD s'applique, émises par la Commission européenne, conformément à l'article 46, paragraphe 2, du RGPD), ou si
- la protection adéquate des données est assurée par d'autres garanties appropriées au sens de la législation applicable en matière de protection des données.

Dans le cas où le client a son siège dans un pays tiers en dehors de la Suisse / de l'UE / de l'EEE, les parties concluront, si nécessaire, un accord séparé garantissant le respect du droit en matière de protection des données applicable au siège du client.

4.3 **Catégories de données personnelles**

Les catégories de données personnelles traitées par Jungheinrich sur ordre du client dépendent du produit numérique Jungheinrich que le client a choisi dans sa page de garde du contrat. Un aperçu des données personnelles traitées dans le cadre du présent contrat peut être consulté dans l'**Annexe 2**.

4.4 **Catégories de personnes concernées**

Les personnes concernées par le traitement des données par Jungheinrich sont décrites dans l'**Annexe 3**.

4.5 **Pas de traitement de données sur ordre**

Dans la mesure où Jungheinrich, dans le cadre de la mise à disposition de ses produits et/ou de la réalisation de ses prestations, collecte et traite (a) des données personnelles relatives à l'utilisation par le client des applications, outils, plates-formes, logiciels ou matériels mis à disposition par Jungheinrich et/ou (b) des données machine non personnelles relatives aux chariots ou machines Jungheinrich utilisés par le client (par ex. données de connexion, données d'utilisation pour la déduction des cycles de maintenance, informations sur la consultation de pages Internet ou de tableaux de bord, données machine des chariots utilisés, etc.), le traitement des données est effectué dans l'intérêt et à des fins propres à Jungheinrich (sécurité informatique, analyse, développement et amélioration de produits). Jungheinrich est responsable de ce traitement de données.

5. **MESURES TECHNIQUES ET ORGANISATIONNELLES**

5.1 Jungheinrich applique, conformément aux instructions correspondantes du client, les mesures techniques et organisationnelles énumérées dans l'**Annexe 5** afin de garantir un niveau de protection adapté au risque du traitement des données en ce qui concerne la confidentialité, l'intégrité, la disponibilité ainsi que la résistance à la charge des systèmes et d'établir la sécurité du traitement des données. Pour ce faire, Jungheinrich prendra en compte l'état actuel de la technique, les coûts d'implémentation ainsi que le type, l'étendue et les buts du traitement ainsi que les différentes probabilités d'occurrence et la gravité des risques pour les droits et les libertés des personnes physiques.

Les mesures techniques et organisationnelles sont soumises aux avancées techniques et au perfectionnement. Jungheinrich est autorisé à mettre en œuvre des mesures

alternatives adéquates dans la mesure où le niveau de sécurité des mesures définies n'est pas inférieur au niveau prescrit. Jungheinrich documentera les principales modifications en adaptant l'**Annexe 5** .

5.2 Dans la mesure où une vérification de l'autorité compétente en matière de protection des données révèle un besoin d'adaptation des mesures techniques et organisationnelles utilisées, les parties mettront en œuvre cette adaptation d'un commun accord dans un délai approprié et Jungheinrich adaptera l'**Annexe 5** en conséquence.

6. POUVOIR D'EDICTER DES DIRECTIVES DU CLIENT

6.1 Dans le cadre de cet accord, Jungheinrich traitera les données personnelles uniquement dans le cadre des conventions passées et selon les directives du client, sauf dans le cas où il est dans l'obligation de traiter les données en raison du droit de la Suisse, de l'UE ou des états membres de l'UE / EEE auquel il est soumis ; dans un tel cas, Jungheinrich informe le client de ces exigences légales avant le traitement, du moment que le droit concerné n'interdit pas une telle annonce en raison d'un intérêt public important. Les directives sont d'abord définies par cet accord et peuvent être ensuite modifiées, complétées ou remplacées par le client par des directives individuelles sous forme écrite ou sous format électronique (texte) aux endroits marqués par Jungheinrich. Toutes les instructions données doivent être documentées par les deux parties et conservées pendant toute la durée de la collaboration.

6.2 Le client confirmera les directives orales par écrit ou sous forme électronique.

6.3 Jungheinrich utilise les données personnelles traitées sur ordre du client pour aucun autre but que les buts convenus et en aucun cas pour des buts personnels ou des buts de tiers. Aucune copie ni double n'est créé sans que le client n'en prenne connaissance. Une exception est faite pour les copies de sécurité si celles-ci sont nécessaires à la garantie d'un traitement conforme des données ainsi que pour les données personnelles nécessaires au respect des obligations légales de conservation.

6.4 Jungheinrich informera immédiatement le client s'il estime qu'une directive est en infraction avec les prescriptions en matière de protection des données. Jungheinrich est habilitée à renoncer à l'exécution de la directive correspondante jusqu'à ce qu'elle ait été confirmée ou modifiée par une personne responsable chez le client.

6.5 Le client garantit que les instructions relatives au traitement des données personnelles données à Jungheinrich sont conformes au droit applicable. Le client exempte Jungheinrich de toute réclamation de tiers découlant du non-respect de cette garantie.

6.6 Le client et Jungheinrich nommeront chacun à l'autre partie les personnes (ainsi que les remplacements concernant ces personnes) qui sont autorisées à donner des instructions ou à recevoir des instructions conformément au présent accord. La désignation s'effectue sous forme de texte ou par écrit par la voie habituelle de communication entre les parties.

6.7 Dès qu'une directive dépasse le cadre des prestations convenues dans le contrat principal, Jungheinrich peut réclamer une rémunération appropriée pour leur réalisation.

6.8 Dans la mesure où Jungheinrich traite des données personnelles sous sa propre responsabilité (voir le point 4.5), Jungheinrich n'est pas liée par les directives du client.

7. RECTIFICATION, SUPPRESSION ET LIMITATION DU TRAITEMENT DES DONNEES PERSONNELLES

7.1 Si une personne concernée fait valoir directement auprès de Jungheinrich l'un de ses droits légaux tels que l'information, la rectification, la suppression, la limitation du traitement, la possibilité de transfert des données, la contestation et la cessation d'une décision basée

exclusivement sur une décision automatisée concernant ses données personnelles traitées par Jungheinrich sur ordre du client (ensemble : « **droits des personnes concernées** »), Jungheinrich transmettra cette demande immédiatement au client. Jungheinrich rectifiera, effacera ou limitera le traitement des données personnelles de la personne concernée faisant valoir ses droits uniquement après une directive documentée du client. La même chose est valable pour l'accomplissement du droit de la personne concernée pour la portabilité des données et de l'information. Cela ne s'applique pas aux éventuels traitements de données effectués par Jungheinrich en vertu d'ordonnances administratives ou judiciaires en rapport avec les droits des personnes concernées.

7.2 Les coûts qui surviennent pour Jungheinrich pour son soutien du client dans la garantie des droits des personnes concernées selon le point 7 doivent être remboursés selon les charges réelles basées sur les conditions convenues entre les deux parties dans le contrat principal.

8. RESPONSABLE DE LA PROTECTION DES DONNEES

8.1 Jungheinrich a désigné, dans la mesure où cela est nécessaire, un responsable à la protection des données qui exerce ses fonctions conformément aux dispositions du droit applicable en matière de protection des données.

8.2 Jungheinrich communiquera au client, sur demande, des informations sur la personne et les coordonnées du responsable à la protection des données. Tout changement de responsable à la protection des données sera communiqué par Jungheinrich au client après information.

9. PRESERVATION DE LA CONFIDENTIALITE

9.1 Lors de l'exécution des travaux sur ordre du client, Jungheinrich ne fait appel qu'à des collaborateurs qui se sont engagés à respecter la confidentialité et qui ont été préalablement familiarisés avec les dispositions du droit applicable en matière de protection des données qui les concernent.

9.2 Le client et Jungheinrich sont dans l'obligation de traiter de manière confidentielle toutes les informations concernant les secrets commerciaux et les mesures de sécurité pour les données de l'autre partie acquises dans le cadre de la relation contractuelle. Les réglementations en matière de confidentialité figurant dans les CGV de Jungheinrich s'appliquent. L'obligation de confidentialité s'applique également en cas d'accès à distance aux données personnelles. Elle reste en vigueur même après la résiliation du présent accord. Si les parties ont conclu un accord de confidentialité distinct, celui-ci prévaut sur la réglementation figurant au point 9.2.

9.3 Les parties sont autorisées à transmettre à des conseillers externes des informations en rapport avec le présent accord ou son exécution, dans la mesure où cela est nécessaire pour remplir des obligations légales ou pour la défense et les poursuites judiciaires et où les conseillers externes sont soumis à des obligations de confidentialité contractuelles ou légales correspondant au moins aux obligations découlant du présent accord.

10. OBLIGATION DE CONTROLE ET DE PREUVE DE JUNGHEINRICH

10.1 Jungheinrich contrôle régulièrement ses processus internes ainsi que les mesures techniques et organisationnelles selon l'**Annexe 5** afin de garantir que le traitement dans son domaine de responsabilité s'effectue conformément aux exigences du droit applicable en matière de protection des données et que la protection des droits des personnes concernées soit garantie.

10.2 Jungheinrich expose les mesures techniques et organisationnelles prises sur demande du client dans le cadre de son pouvoir de contrôle selon le point 12 du présent accord.

11. SOUS-TRAITANCES

11.1 Jungheinrich est en droit de faire appel à des sous-traitants.

11.2 Il existe une relation de sous-traitance lorsque Jungheinrich confie à des sous-traitants l'ensemble ou une partie de la prestation due au client en vertu du contrat principal comprenant un traitement de données personnelles sur ordre du client. Jungheinrich sélectionnera les sous-traitants minutieusement en considérant en particulier les mesures techniques et organisationnelles prises par ceux-ci et conclura avec eux des accords dans l'étendue nécessaire pour garantir des mesures appropriées concernant la protection des données et la sécurité des informations.

11.3 Le client accepte que Jungheinrich fasse appel aux sous-traitants mentionnés dans l'**Annexe 6** . Jungheinrich informe le client avant la participation de sous-traitants supplémentaires ou le remplacement de sous-traitants mentionnés. Le client peut s'opposer à une telle modification des sous-traitants dans un délai de quatorze (14) jours à compter de la notification de la modification. Le client doit justifier son opposition et, en particulier, ne doit pas faire usage de son droit d'opposition de manière arbitraire. Si aucune opposition n'est effectuée durant ce délai, il est considéré que l'accord pour la modification a été donné. Si le client s'oppose à la modification de la sous-traitance et si Jungheinrich n'est pas en mesure de trouver rapidement un autre sous-traitant à des conditions appropriées, Jungheinrich a le droit au choix d'adapter la rémunération convenue aux coûts supplémentaires occasionnés par la sous-traitance alternative ou de résilier le présent accord et le contrat principal de manière exceptionnelle.

11.4 Si Jungheinrich attribue des ordres de commandes à des sous-traitants, Jungheinrich transmet ses obligations concernant le droit en matière de protection des données découlant du présent accord aux sous-traitants selon le droit applicable en matière de protection des données dans l'étendue appropriée. Jungheinrich conclura à cet effet un accord correspondant sous forme de texte avec le sous-traitant et contrôlera régulièrement le respect de ces obligations par le sous-traitant.

11.5 Une relation de sous-traitance au sens de cette réglementation n'existe que pour les prestations de service qui sont fournies au client pour l'exécution de la prestation principale ou qui sont en relation directe avec la prestation principale. Les prestations auxiliaires que Jungheinrich reçoit de tiers dans le cadre de l'exercice de ses propres activités et pour lesquelles les tiers n'ont pas accès aux données personnelles du client, comme par exemple les prestations de télécommunication et de maintenance technique, les services aux utilisateurs et les services de nettoyage, ne sont pas saisies. Toutefois, pour garantir la protection et la sécurité des données personnelles du client, Jungheinrich est tenue de passer des conventions contractuelles appropriées ainsi que de prendre des mesures de contrôle même pour ce type de prestations auxiliaires.

12. DROITS DE CONTROLE DU CLIENT

12.1 En cas de motif justifié, le client a le droit de demander à tout moment, sinon une fois tous les deux ans, en accord avec Jungheinrich et dans l'étendue nécessaire et raisonnable, une preuve du respect du présent accord par Jungheinrich. De manière générale, Jungheinrich prouvera le respect de cet accord par la présentation d'une certification ou d'autres documents appropriés.

12.2 Dans le cas où la présentation d'une certification ou des autres documents appropriés selon le paragraphe 1 ne suffit pas à prouver le respect du présent accord dans un cas particulier,

Jungheinrich permettra au client, après concertation commune et un délai de notification de trois (3) semaines, de procéder à un contrôle sur place du traitement de l'ordre de commande conformément au présent accord dans les locaux de Jungheinrich aux heures de travail habituelles de Jungheinrich. Le client ne fera effectuer de tels contrôles que par du personnel de vérification interne ou externe suffisamment qualifié et tenu à la confidentialité. Les personnes qui, en raison de leur profession ou de leur relation de travail, doivent être considérées comme des concurrents de Jungheinrich, ne sont pas aptes à effectuer ces contrôles. Jungheinrich ne doit pas autoriser de contrôles effectués par des personnes insuffisamment qualifiées ou inadaptées. Le client informera Jungheinrich au plus tard une (1) semaine avant la date prévue pour le contrôle sur place des personnes devant effectuer le contrôle sur place.

12.3 Le client remboursera à Jungheinrich ses frais occasionnés par l'exercice des droits de contrôle du client à un niveau approprié, sur la base des conditions convenues entre les parties dans le contrat principal en tenant compte des moyens utilisés par Jungheinrich.

12.4 La preuve de mesures ne concernant pas seulement le traitement concret de l'ordre de commande peut être apportée par Jungheinrich à sa discrétion par le respect des règles de conduite (art. 40 RGPD) ; la certification selon une procédure approuvée (art. 13 LDP, art. 42 RGPD) ; des attestations, des rapports ou des extraits de rapports actuels établis par des instances indépendantes (par ex. experts-comptables, révision, préposés à la protection des données, service de la sécurité informatique, experts certifiés en protection des données, contrôleurs qualité) ; une certification appropriée d'un service d'expertise en matière de sécurité informatique ou de protection des données (par ex. selon la protection de base de l'office fédéral de la sécurité des technologies de l'information) ou des mesures comparables. Jungheinrich mettra à la disposition du client, sur demande, une preuve correspondante sous une forme et dans une étendue appropriées.

13. ANNONCE ET COMPORTEMENT DE JUNGHEINRICH EN CAS DE VIOLATION DE LA PROTECTION DES DONNEES

13.1 Jungheinrich informe immédiatement le client s'il a connaissance de violations de la protection des données personnelles du client ou en cas d'autres infractions contre les prescriptions ou les réglementations du présent accord concernant le droit en matière de protection des données. Jungheinrich prend des mesures appropriées pour protéger les donnes personnelles et pour réduire les éventuelles conséquences négatives pour le client ou les personnes concernées et se concerte pour ce faire avec le client.

13.2 Jungheinrich informe immédiatement le client sur les mesures de contrôle et les autres mesures des autorités de surveillance ou d'enquête si celles-ci ont un rapport avec le présent accord, à moins que Jungheinrich ne reçoive l'interdiction d'informer le client par l'autorité chargée de l'enquête. Le client et Jungheinrich collaborent, sur demande, avec l'autorité de surveillance ou d'enquête dans l'accomplissement de leurs tâches.

13.3 Dans la mesure où le client est, de son côté, exposé à un contrôle des autorités de surveillance, à une procédure suite à une infraction ou à une procédure pénale, à une demande de responsabilité d'une personne concernée ou d'un tiers ou à une autre demande en relation avec le traitement de l'ordre de commande par Jungheinrich, Jungheinrich soutiendra le client dans la mesure du possible et dans l'étendue nécessaire et raisonnable dans l'utilisation de la protection juridique contre une mesure de ce type et/ou dans la résistance contre ce type de demandes. Les dépenses survenues auprès de Jungheinrich doivent être remboursées à Jungheinrich dans les conditions définies dans le contrat principal.

13.4 Les présentes régulations sont valables de manière inchangée également après l'expiration du présent accord jusqu'à l'accomplissement complet des obligations définies.

14. SUPPRESSION ET RETOUR DE DONNEES PERSONNELLES

14.1 Jungheinrich permet de manière standard une suppression des données du client conforme à la protection des données dans un délai de six (6) mois après la fin de la durée du présent accord. Le client peut exiger que Jungheinrich lui remette à une date antérieure l'ensemble des documents, des résultats de traitement et d'utilisation créés ainsi que les bases de données en rapport avec la relation contractuelle qui sont entrés en possession de Jungheinrich ou qu'ils soient effacés ou détruits conformément à la protection des données. Si le client fait usage de son droit figurant dans la phrase 2, il devra rembourser à Jungheinrich tous les frais occasionnés à un niveau approprié, sur la base des conditions convenues entre les parties dans le contrat principal.

14.2 Jungheinrich est en droit de conserver des copies des documents entrés en sa possession, des résultats de traitement et d'utilisation créés ainsi que des bases de données, si et dans la mesure où cela est nécessaire pour satisfaire aux obligations légales de conservation de Jungheinrich (par ex. en vertu du droit fiscal ou à des fins de comptabilité et de facturation) ou pour faire valoir, exercer ou défendre des droits juridiques.

15. AUTRES OBLIGATIONS DE JUNGHEINRICH

Sur demande du client par écrit ou sous forme de texte, Jungheinrich est dans l'obligation d'apporter son soutien et sa collaboration dans la mesure du raisonnable

(a) lors de l'exercice des droits des personnes concernées,

(b) lors de l'évaluation de l'impact sur la protection des données du client,

(c) dans le cadre de consultations préalables avec l'autorité de surveillance ainsi que

(d) lors de l'établissement du registre de traitement par le client

dans l'étendue requise par le droit applicable en matière de protection des données. Même en cas de coopération ou de soutien du client par Jungheinrich, le client reste seul responsable et redevable des actes ou de la documentation mentionnés aux points (a) à (d).

Jungheinrich peut réclamer pour les prestations de soutien nommées aux points (a) à (d) une rémunération basée sur les tarifs horaires convenus dans le contrat principal.

16. RESPONSABILITE EN CAS DE VIOLATIONS DU DROIT EN MATIERE DE PROTECTION DES DONNEES

Chaque partie est responsable vis-à-vis des personnes concernées conformément au droit applicable en matière de protection des données. Les parties sont responsables du respect de leurs obligations régies par le présent accord conformément aux dispositions légales du droit applicable. Par ailleurs, les règles de responsabilité des CGV de Jungheinrich s'appliquent.

17. DISPOSITIONS FINALES

17.1 Toute modification du présent accord et des accords annexes doit être faite par écrit ou par signature électronique qualifiée. Ceci est également valable pour le renoncement de cette exigence de forme.

17.2 Si certaines parties du présent accord ou de ses modifications ou compléments futurs sont ou deviennent totalement ou partiellement nulles, invalides, contestables ou inapplicables, cela n'affecte pas la validité des autres réglementations de l'accord. La disposition nulle, invalide, contestable ou inapplicable sera remplacée par une réglementation appropriée qui, dans la mesure où cela est juridiquement possible, se

rapproche le plus de ce que les parties auraient voulu si elles avaient su que la disposition était totalement ou partiellement nulle, invalide, contestable ou inapplicable.

17.3 En cas de contradiction entre le présent accord et le contrat principal, les réglementations figurant dans le présent accord en ce qui concerne les obligations relatives au traitement des données personnelles dans le cadre du traitement des données décrit dans l'**Annexe 2**, l'**Annexe 3** et l'**Annexe 4** du présent accord prévalent sur le contrat principal.

18. **LISTE DES ANNEXES**

Les annexes suivantes font partie intégrante du présent accord :

- **Annexe 1** : Modèle de lettre d'adhésion
- **Annexe 2** : Catégories de données personnelles
- **Annexe 3** : Catégories de personnes concernées
- **Annexe 4** : Informations complémentaires sur le traitement des données
- **Annexe 5** : Mesures techniques et organisationnelles
- **Annexe 6** : Sous-traitants

Annexe 1

Annexe 1 – Modèle de lettre d'adhésion

De :

……

……..

À :

……

……..

[*date*]

ADHESION A L'ACCORD SUR LE TRAITEMENT DES ORDRES DE COMMANDES POUR LES PRODUITS NUMERIQUES JUNGHEINRICH

Nous nous référons à l'accord de traitement des commandes pour les produits numériques Jungheinrich (« **Accord** ») du _____[date de conclusion du contrat] entre_____ [insérer la société du client] et _____[insérer la société de la société Jungheinrich avec laquelle le contrat principal a été conclu].

Conformément à la clause 3.2 de l'Accord, nous adhérons par la présente à l'Accord, y compris à toutes les annexes, aux conditions mentionnées dans la clause 3, avec effet à compter du_____ [date d'adhésion].

Pour : _____

[*nom de l'entreprise adhérente*]

Nom : _____

Fonction : _____

Lieu, date : _____

Signature : _____

Annexe 2

Annexe 2 – Catégories de données personnelles

Pour les produits numériques Jungheinrich sélectionnés par le client dans la page de garde du contrat, les catégories de données personnelles suivantes sont traitées :

Catégories de données personnelles	Jungheinrich FMS						
	Starter Kit	Finance Bundle	Access Bundle	Productivity Bundle	Safety Bundle	Safety Bundle Plus	Energy Bundle
Données personnelles de base	x	x	x	x	x	x	x
Données de communication	x	x	x	x	x	x	x
Données de connexion	x	x	x	x	x	x	x
Données des utilisateurs des chariots	x		x	x	x	x	x
Données des chariots	x		x	x	x	x	x
Données médicales					(x)*	(x)*	

Catégories de données personnelles	Jungheinrich FMS						
	Équipement / Site / Contrats API	Coût d'exploitation API	Engagement horaire API	Gestion de crise API	Utilisations API	Collaborateur API	Contrôle d'accès API
Données personnelles de base						x	x
Données de communication	x	x	x	x	x	x	x
Données de connexion	x	x	x	x	x	x	x
Données des utilisateurs des chariots	x		x	x	x	x	x
Données des chariots	x		x	x	x	x	x

Les catégories de données susmentionnées comprennent en règle générale les données suivantes qui peuvent être mises à disposition par le client et traitées par Jungheinrich pour la fourniture des prestations :

- Données personnelles de base (par ex. prénom, initiale du deuxième prénom, nom de famille, signature, numéro personnel)
- Données de communication (p. ex. adresse e-mail de connexion, adresse e-mail alternative, adresse, numéro de téléphone, clé API)
- Données de connexion (p. ex. protocoles des heures de connexion et de déconnexion effectuées ainsi que des heures de saisie et de modification, adresse IP, modifications de la configuration dans le portail de gestion, date et heure de connexion et de déconnexion d'un cariste à un chariot donné, y compris l'état final du chariot, Multilogin)
- Données des utilisateurs des chariots (par ex. prénom, nom, identifiant du transpondeur, catégorie de permis de conduire, numéro de permis, date de délivrance, date d'expiration, niveau d'expérience du cariste, informations de connexion, identifiant d'accès, PIN, identifiant externe, permission, taux horaire, expiration de la certification, date d'expiration du permis, affectation de groupe, temps de conduite, messages de chocs du chariot conduit)

- Données des chariots (par ex. identifiant du chariot, segment du chariot, vitesse, événements de levage (levée et descente), niveau de charge de la batterie, type de chariot, utilisations, chocs, nombre total de chocs pendant l'utilisation, listes de contrôle remplies par les caristes, résultat du contrôle de démarrage sur l'état du chariot)

- Géolocalisation (par ex. localisation WiFi, localisation GPRS)

- Données médicales (* Module Pre-Op Check : par défaut, aucune liste de contrôle n'est prédéfinie par le système, aucun traitement de données médicales n'est donc prévu. Les clients peuvent créer et utiliser des listes de contrôle individuelles à leur convenance. Cela ne peut exclure la collecte et le traitement de données médicales, qui s'effectuent donc sous la propre responsabilité du client, conformément au point 1.8 de la convention. Pour plus d'informations, veuillez consulter l'annexe 4 pièce jointe A de la convention.)

Les produits numériques Jungheinrich mis à disposition par Jungheinrich sont régulièrement adaptés et mis à jour en fonction des nouvelles exigences techniques et juridiques. Cela peut entraîner des changements dans les catégories de données personnelles traitées dans les différents packs de produits numériques Jungheinrich. Un aperçu actualisé des catégories de données traitées peut être consulté via le lien suivant : https://jungheinrich.com/processing-of-personal-data-in-jungheinrich-digital-products-1136138.

Annexe 3

Annexe 3 – Catégories de personnes concernées

Pour les produits numériques Jungheinrich sélectionnés par le client dans la page de garde du contrat, les catégories de personnes concernées suivantes sont traitées :

Catégories de personnes concernées	Jungheinrich FMS						
	Starter Kit	Finance Bundle	Access Bundle	Productivity Bundle	Safety Bundle	Safety Bundle Plus	Energy Bundle
Utilisateurs(trices)	x	x	x	x	x	x	x
Caristes			x	x	x	x	x
Signataires de rapports de service		x					

Catégories de personnes concernées	Jungheinrich FMS API							
	Équipement / site API	Contrats API	Coût d'exploitation API	Engagement horaire API	Gestion des chocs API	Utilisations API	Collaborateur API	Contrôle d'accès API
Utilisateurs(trices)	x	x	x	x	x	x	x	x
Caristes	x				x	x	x	x

Les produits numériques Jungheinrich mis à disposition par Jungheinrich sont régulièrement adaptés et mis à jour en fonction des nouvelles exigences techniques et juridiques. Cela peut entraîner des changements dans les catégories de personnes concernées dans les différents produits numériques Jungheinrich. Un aperçu actualisé des catégories de personnes concernées peut être consulté via le lien suivant : https://jungheinrich.com/processing-of-personal-data-in-jungheinrich-digital-products-1136138.

Annexe 4

Annexe 4 – Informations complémentaires sur le traitement des données

Les produits numériques Jungheinrich proposés par Jungheinrich peuvent être commandés avec différents packs de prestations (« **Bundles** »). La sélection des packs s'effectue dans la page de garde du contrat du client correspondant. Cette **annexe 4** contient des informations complémentaires sur le traitement des données pour chaque produit numérique Jungheinrich, notamment sur le type et le but du traitement des données ainsi que sur les catégories de données personnelles et de personnes concernées. Les détails concernant le traitement des données pour chaque produit numérique Jungheinrich figurent dans les pièces jointes de la présente **annexe 4**. Un aperçu des catégories de données traitées dans les différents packs figure dans l'**Annexe 2**, un aperçu des catégories de personnes concernées par le traitement des données dans le cadre de chaque pack figure dans l'**Annexe 3**.

Pièce jointe concernant l'annexe 4	**Produit numérique Jungheinrich**
Annexe A	Système de gestion de flotte Jungheinrich (« **Jungheinrich FMS** »)
	Starter Kit
	Finance Bundle
	Access Bundle
	Safety Bundle
	Productivity Bundle
	Safety Bundle Plus
	Energy Bundle
Pièce jointe B	Jungheinrich FMS Application Programming Interface (« **API** »)
	Équipement / site / contrats API
	Coût d'exploitation API
	Heures de service API
	Gestion des chocs API
	Utilisations API
	Collaborateurs API
	Contrôle d'accès API
Les produits numériques Jungheinrich suivants ne traitent aucune donnée personnelle sur ordre. Jungheinrich est responsable des produits numériques Jungheinrich mentionnés ci-dessous. La liste fournit un aperçu de tous les produits numériques Jungheinrich.	
Annexe C	Call4Service

Annexe 4 pièce jointe A

Pièce jointe A – Jungheinrich FMS

Type et buts du traitement

Dans le cadre de la mise à disposition du Jungheinrich FMS, Jungheinrich traite les données personnelles mises à disposition par le client ou collectées pour le client durant la réalisation des prestations ou traitées d'une manière diverse dans les buts mentionnés ci-dessous sur son ordre.

Le traitement des données personnelles des utilisateurs(trices) du portail en ligne Jungheinrich FMS mis à disposition par Jungheinrich, qui a lieu dans le cadre de l'utilisation du portail, n'est pas saisi par le traitement des ordres de commandes. Ce traitement est effectué sous la seule responsabilité de Jungheinrich.

Lors de l'utilisation par le client du Jungheinrich FMS mis à disposition par Jungheinrich, il existe des données (de machines) qui, dans certaines circonstances, ont un rapport direct à des personnes et sont ainsi soumises dans ce cas aux prescriptions en matière de protection des données. Jungheinrich collecte et enregistre ces données sur ordre du client afin de permettre l'utilisation du système de gestion de flotte convenue par contrat. Le but du traitement des données est donc la collecte, l'analyse et l'évaluation des données du client en vue de la commande et de la gestion de sa flotte de chariots.

La saisie de données autres que les données concernées et citées dans la présente pièce jointe n'est pas requise, mais peut être effectuée par le client sous sa propre responsabilité. Dans ce cas, le client est le seul responsable de la garantie de la légalité du traitement des données par des mesures appropriées en interne avec ses collaborateurs.

Le Jungheinrich FMS est divisé en différents packs (Bundles) qui sont acquis individuellement par le client. Les buts respectifs ainsi que les données traitées dans chaque cas sont décrits pour chaque pack ci-après.

Catégories de données personnelles

Les catégories de données personnelles concernées par le traitement des données dans le cadre des différents packs figurent dans l'**Annexe 2**.

Catégories de personnes concernées

Les catégories de personnes concernées par le traitement des données dans le cadre des différents packs figurent dans l'**Annexe 3**.

Packs (Bundles) du Jungheinrich FMS

1. **Starter Kit**

   Type et buts du traitement

   Le Starter Kit contient une fonction d'inventaire servant à la numérisation des entrepôts. Il fournit ainsi une plate-forme pour la numérisation des entrepôts. Il permet d'attribuer et de gérer des numéros de série internes et des noms d'appareils et d'ajouter des appareils supplémentaires.

   La fonction heures de service du Starter Kit permet une optimisation de l'utilisation de la flotte. Cela se fait sur la base de prévisions au niveau de la flotte, des chariots et des données contractuelles.

En attribuant des chariots et des appareils à des utilisateurs(trices) individuel(le)s et à des groupes d'utilisateurs(trices) ou à des caristes et à des groupes de caristes, une référence personnelle peut être établie dans certaines circonstances.

2. **Finance Bundle**

Type et buts du traitement

Le Finance Bundle offre de la transparence en affichant les coûts des chariots individuels ainsi que ceux de l'ensemble de la flotte sur une période choisie par l'utilisateur. La fonction d'analyse détermine les coûts respectifs par heure de service et les affiche sur des périodes de temps sélectionnables individuellement et des tendances historiques au sein du module Coûts d'exploitation du Finance Bundle. Les factures, les rapports de service et les données des chariots sont pris en compte pour l'analyse. Celles-ci contiennent généralement des données personnelles. En outre, ce package offre de la transparence sur les rapports de service des différents chariots. Il permet ainsi d'avoir une vue d'ensemble sur les services effectués pour la flotte. De plus, le bundle affiche un aperçu des services de maintenance à venir et passés. En outre, le package offre la possibilité de suivre visuellement les écarts de coûts par la définition des seuils individuels à surveiller.

3. **Access Bundle**

Type et buts du traitement

L'Access Bundle est utilisé pour protéger la flotte contre toute utilisation non autorisée. Les chariots sont mis en marche par l'intermédiaire d'une carte transpondeur. Il est possible de définir individuellement pour chaque cariste quels chariots peuvent être utilisés avec une carte transpondeur définie. L'autorisation peut se référer au permis de conduire, à l'affectation du poste de travail et au type de chariot.

La fonction interventions des caristes donne un aperçu de l'utilisation de la flotte de chariots élévateurs. Les chariots sont mis en service par l'intermédiaire d'une carte transpondeur. L'aperçu est constitué des heures de mise en marche et d'arrêt des chariots qui sont enrichies d'informations supplémentaires, à savoir des données sur les utilisateurs(trices) du chariot et sur le chariot, afin de fournir à l'utilisateur(trice) une vue d'ensemble de l'utilisation de la flotte de chariots et de détecter d'éventuelles utilisations non autorisées. Il est possible de déterminer pour chaque utilisation du chariot le/la cariste respectif(ve) et la carte transpondeur correspondante.

La fonction de contrôle de démarrage est utilisée pour effectuer les demandes d'état des chariots élévateurs par le/la cariste dans le but d'augmenter la sécurité dans l'entrepôt. En fonction des composants montés dans les chariots, des demandes à un niveau (contrôle visuel) ou à deux niveaux (contrôle visuel et fonctionnel) sont possibles. Le contrôle de démarrage peut être activé individuellement pour chaque chariot élévateur et s'effectue après une inscription réussie au moyen d'une carte transpondeur sur un afficheur du chariot élévateur concerné. En cas de contrôle de démarrage négatif, par ex. en raison d'un défaut constaté, le système ne restreint pas l'utilisation du chariot élévateur concerné pour le/la cariste.

Tous les contrôles de démarrage effectués sont affichés dans un aperçu, y compris le résultat respectif (« succès » ou « échec »). L'historique des contrôles de démarrage effectués est enrichi d'informations supplémentaires (par ex. l'heure, le numéro de chariot, l'identifiant du/de la cariste) afin d'identifier à temps les défauts des chariots et d'éviter les dommages consécutifs ou les risques pour la sécurité des collaborateurs(trices). Les collaborateurs(trices) ayant effectué le contrôle de démarrage d'un chariot élévateur sont affiché(e)s sans attribution nominative dans le réglage standard. Le client peut également sélectionner dans les paramètres un affichage avec un nom clair.

4. **Safety Bundle**

Type et buts du traitement

Le Safety Bundle comprend les modules Gestion des chocs et Pre-Op Check et aide les clients à augmenter la sécurité dans l'entrepôt.

Le module Gestion des chocs met à disposition des données sur les chocs du chariot et propose des réactions configurables du chariot (p. ex. vitesse lente). Le module Pre-Op Check permet de configurer des listes de contrôle pour l'inspection visuelle et fonctionnelle des chariots, y compris les réactions du chariot (p. ex. vitesse lente). Les listes de contrôle peuvent être attribuées à des chariots individuels et le/la cariste doit y répondre sur le chariot à des moments configurables. La réponse à la liste de contrôle se fait à la suite d'une procédure d'enregistrement réussie par le/la cariste au moyen d'une carte transpondeur et constitue une condition préalable à la disponibilité opérationnelle du chariot. Les résultats des requêtes d'état sont enrichis de données supplémentaires (p. ex. heure, numéro de chariot, identifiant du/de la cariste) et sont mis à disposition dans un rapport sur le portail FMS. Une vue détaillée permet de consulter les réponses aux différentes questions des listes de contrôle. Par défaut, les protocoles des contrôles de démarrage sont affichés sans attribution nominative. Le client peut également sélectionner dans les paramètres un affichage avec un nom clair.

Les modules Gestion des chocs et Pre-Op Check sont utilisés conjointement avec le contrôle d'accès. L'Access Bundle est ainsi déjà inclus dans le Safety Bundle.

5. **Productivity Bundle**

Type et buts du traitement

Le Productivity Bundle offre, outre les fonctionnalités d'Access, un aperçu des différentes utilisations de la flotte de chariots élévateurs et de la flotte du client. Le client a la possibilité de visualiser à la fois l'utilisation parallèle et les pics d'utilisation. L'utilisation est déterminée par le traitement des temps d'utilisation des chariots.

6. **Safety Bundle Plus**

Type et buts du traitement

Le Safety Bundle Plus combine les fonctionnalités du Safety Bundle ainsi que du Productivity Bundle. Il met ainsi à disposition des données sur les chocs, permet de créer des listes de contrôle pour vérifier l'état des chariots (Pre-Op Check), propose des réactions configurables des chariots (p. ex. vitesse lente) et permet d'avoir un aperçu des différentes utilisations de la flotte du client. Les données permettant de déterminer l'utilisation se réfèrent aux temps d'utilisation des chariots.

7. Energy Bundle

Type et buts du traitement

L'Energy Bundle fournit des informations pertinentes en matière d'énergie sur la base des valeurs de charge de la batterie des chariots élévateurs électriques équipés d'un boîtier télématique Jungheinrich. Il est ainsi possible d'analyser le modèle d'utilisation actuel des batteries afin d'en déduire les mesures possibles pour maximiser l'efficacité et la durée de vie des batteries. Lorsque la gestion des accès est activée, les données affichées dans ce bundle peuvent potentiellement être attribuées aux utilisateurs du chariot.

Délais de suppression et de stockage

Les périodes de stockage habituelles des données à caractère personnel et des principales données non personnelles sont décrites ci-dessous :

Tableau de la durée de stockage habituelle des données à caractère personnel dans le JH FMS

Données des clients	Durée de stockage	Bundles concernés
Noms des caristes et identifiants des transpondeurs dans les rapports d'intervention	6 mois	Access Bundle, Productivity Bundle, Safety Bundle (Plus)
Noms des caristes et identifiants des transpondeurs dans la gestion des accès	Jusqu'à la fin du contrat ou de la licence ou jusqu'à la suppression manuelle par le client	Access Bundle, Productivity Bundle, Safety Bundle (Plus)
Nom des utilisateurs(trices) connecté(e)s dans les protocoles d'audit	18 mois	Tous les bundles disponibles
Noms des caristes et identifiants des transpondeurs dans les rapports de Pre-Op Check et de contrôle rapide	6 mois	Safety Bundle (Plus)
Noms des caristes et identifiants des transpondeurs dans les rapports de chocs	6 mois	Safety Bundle (Plus)
Nom et signature des signataires dans les rapports de service (fichiers PDF)	Maximum 2 ans et 36 jours. Les fichiers PDF sont disponibles du 1er janvier de l'année précédente jusqu'au jour actuel.	Finance Bundle

Tableau de la durée de stockage habituelle des données à caractère non personnel dans le JH FMS

Données des clients	Durée de stockage	Justification d'une durée de conservation supérieure à 5 ans	Bundles concernés
Rapports Pre-Op Check	2 ans		Safety Bundle (Plus)
Listes de contrôle actives	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit	Safety Bundle (Plus)
Rapports de chocs	2 ans		Access Bundle, Safety Bundle (Plus)
Rapports d'utilisation	2 ans		Access Bundle, Productivity Bundle, Safety Bundle (Plus)
Rapports de service	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit	Finance Bundle
Échéances de maintenance	5 ans		Finance Bundle
Données de base du client (client, équipements, sites, tags (caractéristiques), licence, heures d'ouverture des sites, valeurs limites)	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit	Tous les bundles disponibles
Valeurs limites de productivité : utilisation maximale, utilisation de l'équipement	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit	Productivity Bundle, Safety Bundle (Plus)
Utilisations pour les analyses de la productivité	2 ans		Productivity Bundle, Safety Bundle (Plus)
Valeurs limites des coûts et heures de service : *équipement, site, limite des coûts annuels, limite des heures de service*	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit	Finance Bundle

Sauvegardes techniques du système : Logfiles, données de sauvegarde	6 mois		Tous les bundles disponibles
Heures de service	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit / exigence contractuelle	Tous les bundles disponibles
Données des contrats d'achat, de location, de service	Jusqu'à l'expiration du contrat	Nécessaire pour la mise à disposition du produit / exigence contractuelle	Starter Kit, tous les bundles disponibles
Coûts (y compris les factures et les postes de facturation, ainsi que les factures générées par les utilisateurs)	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition du produit	Finance Bundle
Données de la batterie et de la charge	2 ans		Energy Bundle

En option, s'il existe un accord contractuel sur l'utilisation du FMS API (interface) :

Données des clients	**Durée de stockage**	**Justification d'une durée de conservation supérieure à 5 ans**	**Catégories API concernées**
Données de base FMS API : client, sites, équipements, tags (caractéristiques), licences	Jusqu'à la fin du contrat ou de la licence	Nécessaire pour la mise à disposition de l'interface / API	Toutes les catégories API disponibles
Gestion des clés API (y compris les journaux d'audit)	Jusqu'à l'expiration de la licence	Nécessaire pour la mise à disposition de l'interface / API	Toutes les catégories API disponibles

Annexe 4 pièce jointe B

Pièce jointe B – Jungheinrich FMS API

Type et but du traitement

Sur instruction du client, Jungheinrich fournit des données à caractère personnel qui seront traitées dans le cadre de la mise à disposition du Jungheinrich FMS au client conformément à la **pièce jointe B** de l'**annexe 4** via le Jungheinrich FMS API.

La mise à disposition de données à caractère personnel via le Jungheinrich FMS API s'effectue dans différentes catégories API, qui peuvent être achetées séparément par le client et qui ont des exigences différentes pour les bundles correspondants, qui constituent une condition préalable pour l'API en question. Les buts respectifs ainsi que les données traitées sont décrits ci-dessous pour chaque catégorie API.

Catégories de données personnelles

Les catégories de données personnelles concernées par le traitement dans le cadre de chaque catégorie API sont énumérées dans la **pièce jointe 2**.

Catégories de personnes de concernées

Les catégories de personnes concernées par le traitement des données dans le cadre de chaque catégorie API sont énumérées dans la **pièce jointe 3**.

Catégories API du Jungheinrich FMS

1. **Équipement / site / contrats API**

   Type et but du traitement

   L'API d'équipement récupère des données sur tous les chariots qui se trouvent actuellement sur le site demandé. Un chariot est un élément de la flotte actuellement affecté à un site. L'enregistrement se compose d'un numéro de série, d'un segment, d'une année de construction et d'autres champs qui fournissent des informations détaillées sur l'équipement spécifique.

   L'API de site récupère des données sur les sites avec des informations telles que l'adresse, le code postal, etc.

   L'API des contrats récupère les informations contractuelles pour les chariots situés sur le site indiqué : type de contrat, numéro de contrat, dates de début et de fin, nombre d'heures de service convenu, types de location et autres informations liées au contrat. Un même chariot peut faire l'objet de plusieurs contrats.

   Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API et l'adresse IP peuvent être suivies par Jungheinrich.

2. **Coût d'exploitation API**

   Type et but du traitement

   Le coût d'exploitation API récupère le coût d'un chariot sur le site indiqué pendant la période indiquée. Le bloc de données renvoyé est une liste d'entrées, chaque entrée étant associée à un chariot spécifique.

Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API et l'adresse IP peuvent être suivies par Jungheinrich.

3. Engagement horaire API

Type et but du traitement

L'engagement horaire API récupère toutes les heures de service mesurées d'un chariot sur un site donné avec le paramètre location_id et pour des périodes données. Une mesure des heures de service est un enregistrement des heures de service actuelles d'un chariot donné, mesurées en heures, y compris un horodatage indiquant quand la mesure a été enregistrée. En outre, les mesures peuvent être consultées pour tous les chariots qui sont ou ont été affectés au site indiqué, pour des périodes données.

Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API et l'adresse IP peuvent être suivies par Jungheinrich.

4. Gestion de crise API

Type et but du traitement

La Gestion de crise API récupère toutes les données télémétriques pertinentes d'un événement de choc pour un site donné en utilisant le paramètre location_id. Un événement de choc est envoyé par un chariot qui subit une force importante, p. ex. en heurtant un autre objet ou en subissant une secousse du sol. Outre l'intensité, enregistrée en deux dimensions, la réaction du chariot est également affichée. Les réactions possibles du chariot sont par exemple la vitesse lente ou le blocage du chariot.

Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API, l'adresse IP et les modifications de configuration dans le portail de gestion peuvent être suivies par Jungheinrich.

Les événements de choc sont enrichis d'informations supplémentaires (p. ex. horodatage, numéro de chariot, ID de transpondeur) afin d'identifier à temps des schémas peu sûrs dans le déroulement des opérations et d'éviter des dommages consécutifs ou des risques pour la sécurité des collaborateurs. Les collaborateurs qui effectuent chaque intervention sur un chariot peuvent être identifiés grâce aux données fournies dans l'API de gestion de crise et l'API des collaborateurs.

5. Utilisations API

L'API d'utilisation récupère des données telles que la date et l'heure de début et de fin de l'utilisation, la durée d'utilisation, les heures d'activation et de désactivation du chariot, etc. Les données de l'API d'utilisation offrent aux utilisateurs un aperçu global de l'utilisation de la flotte et permettent de détecter d'éventuels abus. Les données d'utilisation sont enrichies d'informations supplémentaires (p. ex. horodatage, numéro de chariot, type de déconnexion, connexion multiple, ID de transpondeur) afin d'identifier rapidement les cas d'abus et d'éviter les dommages consécutifs ou les risques pour la sécurité des collaborateurs ainsi qu'une utilisation non optimale du chariot. Les collaborateurs qui utilisent un chariot peuvent être identifiés à l'aide des données d'utilisation et de collaborateurs issues des API respectives.

Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API, l'adresse IP ainsi que la date et l'heure de connexion et de déconnexion d'un cariste à un chariot donné peuvent être suivies par Jungheinrich.

6. Collaborateurs API

L'API des collaborateurs récupère les données des collaborateurs sur un site précis : ID d'employé, prénom, nom de famille, ID du transpondeur, rôle, etc. L'attribution de chariots et de dispositifs à des opérateurs et groupes d'opérateurs individuels ou à des caristes et groupes de caristes peut permettre d'établir une relation avec une personne physique identifiée ou identifiable.

Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API et l'adresse IP peuvent être suivies par Jungheinrich.

7. Contrôle d'accès API

Type et but du traitement

L'API de contrôle d'accès récupère les données de configuration d'accès pour un chariot donné (via le paramètre « vehicle_id ») sur un site donné (via le paramètre « location_id »). La configuration d'accès d'un chariot fournit des configurations pertinentes du chariot (p. ex. durée du temps mort) et permet d'activer / désactiver l'accès. Elle contient également des informations sur le moment où une configuration a été envoyée au chariot et sur le moment où elle a été validée par le chariot. Il existe une configuration par défaut qui peut être remplacée, p. ex. en envoyant des demandes de poste API. Une configuration mise à jour est confirmée par le chariot.

L'API de contrôle d'accès est utilisée pour configurer un accès à un chariot et protéger la flotte contre toute utilisation non autorisée sans utiliser l'interface utilisateur du Jungheinrich FMS. Les chariots sont mis en marche avec une carte transpondeur. Il est possible de définir individuellement quels chariots peuvent être utilisés avec une carte transpondeur pour un(e) seul(e) cariste. L'autorisation peut se référer au permis de conduire, à l'affectation du travail et au type de chariot.

En outre, cette API permet au client de créer, de récupérer, de mettre à jour et de supprimer des collaborateurs sur un site donné.

Pour accéder aux données d'un site spécifique et récupérer des données, le client doit utiliser une clé API qui est créée pour le client. La clé API et l'adresse IP peuvent être suivies par Jungheinrich.

Annexe 4 pièce jointe C

Pièce jointe C – Call4Service

Aucune donnée personnelle n'est traitée sur ordre.

Des informations sur le traitement peuvent être trouvées dans la déclaration de protection des données du produit correspondant.

Dans le cas où des modifications ultérieures du produit font que Jungheinrich est responsable du traitement de l'ordre de commande au sens des prescriptions en matière de protection des données, la présente **pièce jointe C** de l' **Annexe 4** sera remplacée en conséquence.

Annexe 5

Annexe 5 – Mesures techniques et organisationnelles

Jungheinrich a pris les mesures techniques et organisationnelles (« **TOMs** ») mentionnées ci-dessous afin d'assurer un niveau de protection adapté aux risques pour les droits et libertés des personnes physiques. Jungheinrich soumet à des intervalles réguliers les TOMs à une vérification et à une évaluation de leur efficacité pour assurer la sécurité du traitement et, si nécessaire, adapte les TOMs en conséquence afin de garantir en permanence un niveau de protection élevé.

La liste concerne l'ensemble des produits numériques Jungheinrich. Selon le produit, les TOMs appliquées peuvent varier.

1. Confidentialité

1.1 Contrôle d'accès

Les mesures suivantes permettent de garantir que l'accès au bâtiment et aux pièces dans lesquelles se trouvent les installations de traitement de données, avec lesquelles des données personnelles sont traitées ou utilisées, est refusé aux personnes non autorisées :

- procédé fiable d'attribution et de transmission d'autorisations d'accès au bâtiment, aux bureaux et aux centres informatiques
- système de contrôle d'accès (carte d'accès)
- gestion centrale des clés
- cartes d'employé avec photo
- conception des centres informatiques en tant que secteurs de sécurité fermés
- verrouillages électroniques à code des pièces des installations de traitement de données
- directive d'accompagnement de visiteurs
- protocoles des personnes entrantes et sortantes
- protection par un service de surveillance (protection du bâtiment en-dehors des heures de bureau)
- système d'alarme anti-intrusion
- vidéo-surveillance dans les centres informatiques et/ou dans les zones sensibles du bâtiment
- entrée sécurisée
- fenêtres anti-intrusions
- fermeture des armoires et des bureaux en cas d'absence

1.2 Contrôle d'accès

Mesures visant à empêcher l'utilisation des systèmes de traitement des données par des personnes non autorisées :

- accès uniquement après identification et authentification
- procédé fiable d'attribution d'autorisations d'accès

- affectation explicite de comptes utilisateur à des utilisateurs
- directive d'utilisation sûre et correcte des mots de passe
- blocage automatique du compte utilisateur après un nombre défini de tentatives de connexion échouées ou après une inactivité définie
- blocage automatique de l'ordinateur après une inactivité définie précédant une nouvelle connexion
- mode veille automatique des ordinateurs locaux
- protocole des accès et analyse des fichiers de protocole si besoin
- suppression contrôlée des données personnelles après expiration de l'accord
- analyse régulière des points faibles pour les applications web
- régulation des installations de traitement et des supports de données mobiles (cryptage des disques durs / des supports de données, directive sur l'utilisation des appareils / supports de données mobiles, possibilité d'éteindre les smartphones à distance)

1.3 **Contrôle d'accès**

Mesures garantissant que les personnes habilitées à utiliser un système de traitement de données ne puissent qu'accéder aux données soumises à leur autorisation d'accès et que les données à caractère personnel ne puissent être lues, copiées, modifiées ou supprimées de manière illicite lors du traitement, de l'utilisation et après l'enregistrement :

- établissement d'un concept d'attribution des rôles et des autorisations
- procédé fiable d'attribution d'autorisations d'accès
- contrôle régulier des autorisations existantes
- protocole des accès et analyse des fichiers de protocole
- concept clair pour les dossiers (convention claire pour les noms de dossiers)
- adaptation des réglages par défaut déterminants pour la sécurité des nouveaux systèmes informatiques et des applications et désactivation des programmes et fonctions déterminants pour la sécurité non utilisés
- désignation claire et conservation sûre des supports de données
- suppression sûre des données
- clear desk / clear screen policy
- archivage des données avec sécurité d'accès
- les données personnelles sensibles sont enregistrées de manière verrouillée selon les normes de sécurité classiques

1.4 **Contrôles de la séparation**

Mesures garantissant que les données prélevées pour des raisons diverses soient traitées de manière séparée :

- séparation logique par réglementations d’accès
- capacité de mandant côté logiciel
- accès aux blocs de données uniquement par l'intermédiaire d'applications répondant à l'obligation de séparation
- séparation des systèmes de production et de test
- connexion de blocs de données avec un but précis

1.5 Pas d’attribution nominative

Mesures garantissant qu’aucun rapport direct à des personnes n’est possible avec les données :

- des analyses dans l'application sont possibles « par défaut » sans rapport direct à des personnes
- possibilité d'évaluation sans attribution nominative par le client

2. Intégrité

2.1 Contrôle de la transmission

Mesures garantissant que les données personnelles ne puissent être lues, copiées, modifiées ou supprimées de manière illicite lors de la transmission électronique ou pendant leur transport ou leur enregistrement sur des supports de données et qu’il est possible de savoir sur quels postes est prévue une transmission de données personnelles par des dispositifs de transmission de données personnelles :

- communication verrouillée sur les réseaux non sécurisés selon les normes de sécurité classiques
- élimination fiable des supports de données devenus inutiles
- possibilité de signature électronique pour la communication personnelle par e-mail
- protocoles sur la consultation et sur la transmission de données personnelles
- interdiction d'utiliser du matériel informatique et des logiciels non autorisés
- pas de transmission d'informations à des services informatiques externes (adresses e-mail privées, stockage Cloud non autorisé)
- directives aux collaborateurs(trices) concernant l'impression de documents sensibles
- directives aux collaborateurs(trices) concernant l'utilisation de supports de données

2.2 Contrôle de la saisie

Mesures garantissant qu'il sera ultérieurement possible de contrôler et de constater si et par qui des données à caractère personnel ont été saisies, modifiées ou supprimées dans des systèmes de traitement de données :

- accès aux systèmes de traitement de données uniquement possible après la connexion
- pas de transmission de mots de passe (directive sur les mots de passe)

- directive sur la procédure à suivre en cas de prise de connaissance d'un mot de passe (directive sur les mots de passe)
- protocoles automatiques lors de la saisie, de la modification et de la suppression de données personnelles
- analyse des fichiers de protocole en cas de besoin

3. Disponibilité et résistance à la charge

3.1 Contrôle de la disponibilité

Mesures garantissant que les données personnelles soient disponibles et protégées de toute destruction ou perte fortuite :

- concept de sauvegarde et de reprise documentée avec sauvegarde régulière et conservation des supports de données à l'épreuve des catastrophes
- utilisation de Security Controls, tels que par ex. une protection anti-virus et un pare-feu
- systèmes de stockage redondants
- conservation séparée des données
- protection contre les incendies, les surchauffes, les dégâts des eaux, les surtensions et les coupures de courant dans la pièce du serveur
- mise en œuvre d'une alimentation sans coupure et de groupes d'alimentation de secours
- présence d'un concept en cas d'urgence (y compris contrôle régulier de son efficacité)
- flux de travail fiable d'exécution de mises à jour
- surveillance des systèmes à la recherche de défauts
- suppléance définie (en particulier pour les comptes privilégiés)
- procédé de vérification et d'évaluation régulières

3.2 Gestion de la protection des données

Mesures garantissant que les TOMs prises restent durablement efficaces :

- contrôle régulier des TOMs prises
- analyse des messages et des rapports sur les événements inhabituels
- formation des collaborateurs(trices) sur l'utilisation du matériel informatique et sur le renforcement de la sensibilisation à la sécurité informatique
- formation technique continue et régulière pour les responsables du système informatique et de la protection des données de l'entreprise

3.3 Pré-réglages favorables à la protection des données

Mesures garantissant qu'une conception technique favorable à la protection des données contribue au respect des principes de base de la protection des données et que les données soient traitées uniquement si nécessaire grâce aux pré-réglages favorables à la protection des données :

- privacy by design
    - garantie organisationnelle que les obligations d'annonces et d'informations soient remplies
    - les personnes concernées par le traitement des données peuvent exercer leur droit d'opposition (par ex. en matière de publicité) par le biais de procédures automatisées
- privacy by default
    - pré-réglages favorables à la protection des données concernant la quantité des données personnelles relevées
    - pré-réglages favorables à la protection des données concernant l'étendue du traitement des données
    - pré-réglages favorables à la protection des données concernant le respect des délais d'enregistrement et de suppression

3.4 **Contrôle de l'ordre**

Mesures garantissant que les données personnelles appelées à être traitées sur ordre ne soient traitées que conformément aux directives du client :

- le traitement des données personnelles du client par Jungheinrich a lieu uniquement pour des fins internes dans le cadre de la relation avec le client
- garantie du traitement des données de l'ordre de commande selon les instructions en délimitant les responsabilités entre le client et Jungheinrich
- les modifications mandatées par le client et à exécuter par Jungheinrich sont soumises aux dispositions du contrôle de l'ordre de commande
- les critères préalablement définis pour la sélection de sous-traitants doivent être rigoureusement respectés
- les collaborateurs(trices) de Jungheinrich ont uniquement accès aux informations dont ils ont besoin pour l'exécution de l'ordre de commande
- obligation du personnel de Jungheinrich concernant les principes de base de la protection des données du droit applicable, en particulier la confidentialité des données
- le contrôle de l'exécution du contrat est garanti

4. **Accès à distance**

Les points 1 à 3 de la présente **Annexe 5** s'appliquent également, dans la mesure où ils sont applicables, en cas d'accès à distance aux données personnelles.

Annexe 6

Annexe 6 – Sous-traitants

Sur ordre du client, Jungheinrich sollicite des prestations de tiers qui traitent les données personnelles sur son ordre (« sous-traitants »). Ceux-ci figurent dans l'aperçu ci-dessous.

Sous-traitants (Nom, forme juridique, siège de la société)	**Type de service**	**Produit numérique Jungheinrich**	**Lieu de traitement** (Lieu du traitement des données)
Jungheinrich AG Informationstechnologie Friedrich Ebert Damm 129, 22047 Hambourg, Allemagne	• Hébergement de services (service mise à disposition)	• Jungheinrich FMS	Lieux des serveurs : • Hambourg, Allemagne (Jungheinrich AG IT) • Francfort, Allemagne (Equinix Germany GmbH)
Jungheinrich Digital Solutions AG & Co.KG Sachsenstr. 20, 20097 Hambourg, Allemagne	• Développement • Maintenance & assistance • Administration informatique	• Jungheinrich FMS	
Jungheinrich Digital Solutions S.L. Calle Gran Via nº 30 - Planta 7, 28013 Madrid, Espagne	• Développement • Maintenance & assistance • Administration informatique	• Jungheinrich FMS	
Jungheinrich Business Services Romania S.R.L. Brasov, Saturn Blvd. N° 51, 5th floor, 105440 Brasov county, Roumanie	• Administration informatique • Support	• Jungheinrich FMS	
Jungheinrich Business Services Croatia d.o.o. Slavonska avenija 1C 10000 Zagreb, Croatie	• Développement • Maintenance & assistance • Administration informatique	• Jungheinrich FMS	
Jungheinrich Svenska AB Starrvägen 16 232 61 Arlöv, Suède	• Développement • Maintenance & assistance • Administration informatique	• Jungheinrich FMS	
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	• Hébergement de services (service mise à disposition)	• Jungheinrich FMS	Lieux des serveurs : • Francfort, Allemagne • Dublin, Irlande • Paris, France • Stockholm, Suède • Milan, Italie
Splunk Services Germany GmbH Salvatorplatz 3, 80333 Munich, Allemagne	• Enregistrement et traitement de données de connexion	• Jungheinrich FMS	Lieu des serveurs : • Francfort, Allemagne
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park,	• Hébergement de services (mise à disposition de services intégrés, en particulier pour le contrôle d'accès et	• Jungheinrich FMS	Lieux des serveurs : • Germany West Central (Allemagne) • West Europe (Pays-Bas) • North Europe (Irlande)

Annexe 6

Leopardstown, Dublin, Irlande	l'analyse et l'évaluation des données)		
Device Insight GmbH Willy-Brandt-Platz 6, 81829 Munich, Allemagne	• Service IoT (mise à disposition interface IoT)	• Jungheinrich FMS	
ClickHouse, Inc. 650 Castro St., Suite 120 #92426, Mountain View CA 94041, USA	• Analyse et évaluation des données basées sur le cloud	• Jungheinrich FMS	Lieu des serveurs : • Francfort, Allemagne