**Accord de traitement des données**

(« CTD »)

**Table des matières**



**CTD liste des Annexes:**

| | |
|---|---|
| **CTD-Annexe I** | **Description du traitement** |
| **CTD-Annexe II** | **Mesures techniques et organisationnelles** |
| **CTD-Annexe III** | **Liste des sous-traitants agréés** |

**Préambule**

Le présent contrat sur le traitement des données (« **CTD** ») est inclus dans le contrat de fourniture des produits ATOSS sur site et d'un SERVICE CLOUD ATOSS (ci-après dénommés individuellement et ensemble « **PRODUITS ATOSS »**) ainsi que d'autres services et prestations connexes (ci-après dénommés également « **CONTRAT »**). Ce CTD fait donc en même temps partie intégrante d'un contrat conclu par écrit (également sous forme électronique) entre la société ATOSS contractante (en tant que sous-traitant - ci-après dénommée « **ATOSS »**) et le CLIENT. ATOSS et le CLIENT sont ci-après dénommés ensemble les « **PARTIES »** ou individuellement la « **PARTIE »**. Les PARTIES conviennent que le CLIENT peut également autoriser ses ENTREPRISES LIÉES à utiliser les PRODUITS ATOSS sous licence conformément aux dispositions du CONTRAT concerné. Étant donné que, dans un tel cas, des données à caractère personnel d'ENTREPRISES LIÉES du CLIENT sont également traitées par ATOSS, le présent CDT s'applique aux scénarios suivants :

- Le CLIENT est le seul responsable en ce qui concerne les données à caractère personnel qui sont rendues accessibles à ATOSS pour le traitement des données.
- Outre le CLIENT, ses ENTREPRISES LIÉES utilisent également les PRODUITS ATOSS sous

licence ; le CLIENT et ses ENTREPRISES LIÉES sont chacun responsables, seuls ou conjointement.

- Le CLIENT est responsable de ses propres données à caractère personnel et sous-traitant des données à caractère personnel de ses ENTREPRISES LIÉES. Du point de vue de ses ENTREPRISES AFFILIÉES, ATOSS est un sous-traitant du CLIENT.
- Le CLIENT n'est que le sous-traitant de ses ENTREPRISES LIÉES et ATOSS est sous-traitant en ce qui concerne les données à caractère personnel.

Indépendamment des groupes de cas susmentionnés, le CLIENT est toujours l'interlocuteur opérationnel central et direct d'ATOSS dans le cadre du présent CTD. Dans la mesure où ATOSS traite des données à caractère personnel dans ce contexte, les conditions du présent CTD s'appliquent.

Pour la mise à disposition des PRODUITS ATOSS conformément au CONTRAT, le recours à des sous-traitants est nécessaire. À cet égard, le CLIENT est conscient qu'ATOSS ne peut pas fournir les PRODUITS ATOSS sans sous-traitants. Le recours aux sous-traitants est régi par le point 6 du présent CTD.

Note sur la neutralité du genre : Les formulations choisies s'appliquent sans restriction aux autres sexes.

## § 1 Objet du présent CTD

1. Objectif et champ d'application : Le présent CTD vise à garantir le respect de l'art. 28, paragraphes 3 et 4, du RGPD.

   Les PARTIES mentionnées dans le CONTRAT ont accepté le présent CTD afin de garantir le respect de l'article 28, paragraphes 3 et 4, du RGPD.

   Le présent CTD s'applique au traitement des données à caractère personnel conformément à l'annexe I du CTD.

   Les annexes I à III du CTD font partie intégrante du présent CTD.

   Si les termes définis dans le RGPD sont utilisés dans le présent CDT, ces termes ont la même signification que dans le règlement concerné.

   Pour le reste, les définitions figurant dans le CONTRAT s'appliquent mutatis mutandis dans le présent CTD.

   Le présent CTD doit être interprété à la lumière des dispositions du RGPD. Le présent CTD ne doit pas être interprété d'une manière qui serait contraire aux droits et obligations prévus par le RGPD ou qui porterait atteinte aux droits ou libertés fondamentaux des personnes concernées.

2. Obligations du CLIENT : Le présent CTD s'applique sans préjudice des obligations du responsable du traitement en vertu du RGPD.

## § 2 Description du traitement

Les PARTIES conviennent de l'étendue concrète des prestations dans le CONTRAT. Les prestations à prendre en considération englobent régulièrement des faits au sens du traitement de données à caractère personnel pour le compte de tiers. Cela s'applique également au (télé)contrôle et à la (télé)maintenance de procédures automatisées ou à l'utilisation d'installations de traitement de données, dans la mesure où l'accès à des données à caractère personnel du CLIENT ne peut être exclu dans ce cadre.

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées en sous-traitance, sont précisés à **l'CDT-Annexe I - Description du traitement.**

**§ 3 Mesures techniques et organisationnelles**

1. Garantie de la sécurité des données : ATOSS doit respecter les principes d'un traitement régulier des données et veiller à leur respect (cf. art. 5 du RGPD). ATOSS s'engage à respecter les dispositions de l'art. 28, paragraphe 3, point c), 32 du RGPD. ATOSS a pris des mesures appropriées en matière de sécurité des données et garantit un niveau de protection adapté au risque en matière de confidentialité, d'intégrité, de disponibilité et de résistance des systèmes, en procédant en permanence aux adaptations nécessaires. Pour déterminer le niveau de protection adéquat, il convient de tenir compte des risques liés au traitement effectué en sous-traitance, notamment la destruction, la perte ou l'altération, accidentelle ou illicite, ou la divulgation non autorisée de données à caractère personnel transmises, stockées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. Il convient de tenir compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée et des finalités du traitement, ainsi que des différents degrés de probabilité et de gravité du risque pour les droits et libertés des personnes physiques.

2. Documentation et présentation des mesures : ATOSS prend au moins les mesures techniques et organisationnelles mentionnées dans le **CTD-Annexe II - Mesures techniques et organisationnelles**, afin de garantir la sécurité des données à caractère personnel.

3. État actuel de la technique et adaptations techniques : Les mesures techniques et organisationnelles sont soumises au progrès et au développement techniques. Dans ce contexte, ATOSS est autorisé à mettre en œuvre des mesures alternatives adéquates. Ce faisant, il convient d'atteindre le niveau de sécurité des mesures définies dans le présent CTD. Les modifications importantes des mesures techniques et organisationnelles doivent être documentées et notifiées au CLIENT de manière appropriée (par ex. par e-mail ou via un portail en ligne accessible via le site Internet d'ATOSS). Par cette notification, ATOSS donne au CLIENT la possibilité de s'opposer à ces modifications par écrit dans un délai de six (6) semaines. Le CLIENT n'a le droit de s'y opposer que si les modifications ne répondent pas aux exigences de l'art. 3, point 1 et l'art. 3 point 2 du présent CTD. Si le CLIENT ne s'oppose pas ou ne s'oppose pas de manière justifiée aux modifications dans le délai d'opposition, l'acceptation des modifications est réputée acquise à l'expiration du délai. En cas d'opposition justifiée, ATOSS peut suspendre la partie de la prestation de services concernée par l'opposition justifiée du CLIENT.

**§ 4 Pouvoir de donner des instructions**

1. Instruction documentée : ATOSS ne traitera les données à caractère personnel du CLIENT que sur instruction documentée du CLIENT, à moins qu'ATOSS ne soit légalement tenue de les traiter en vertu du droit de l'Union ou du droit de l'État membre auquel ATOSS est soumis. Dans ce cas, ATOSS communiquera ces exigences légales au CLIENT avant le traitement, à moins que le droit en question ne l'interdise pour un

motif d'intérêt public important. Le CONTRAT, y compris le présent CTD, constitue une instruction documentée du CLIENT.

2. Précision et forme des instructions : Sauf convention contraire expresse dans le présent CTD, les instructions doivent être données de manière déterminée (principe de clarté des instructions). Les instructions doivent être données par écrit.

3. Applicabilité de l'instruction : ATOSS informera le CLIENT par écrit dans un délai raisonnable, à condition que le CLIENT puisse configurer lui-même les instructions dans le cadre des fonctionnalités standards.

   Les instructions du CLIENT qui ne correspondent pas aux prestations définies dans le CONTRAT ou dans le présent CTD sont considérées comme une demande de modification du contrat.

   Les obligations découlant du CONTRAT et du présent CTD ne sont pas affectées pendant la période d'audit. ATOSS s'efforcera, dans la mesure du raisonnable, de mettre en œuvre les instructions du CLIENT, pouvant être qualifiées de demande de modification du contrat, dans la mesure où elles sont notamment nécessaires du point de vue de la protection des données et techniquement possibles ou ne nécessitent pas de modifications des PRODUITS ATOSS. ATOSS informera préalablement le CLIENT par écrit si l'examen et la mise en œuvre de la directive entraîneraient un surcroît de travail et/ou des coûts supplémentaires pour ATOSS et, après avoir consulté le CLIENT, lui transmettra une offre pour l'engagement de services payants pour la poursuite de l'examen et de la mise en œuvre de la directive. En l'absence d'un accord sur une modification du contrat, les obligations découlant du CONTRAT demeurent inchangées. Les instructions confirmées par ATOSS sont mises en œuvre dans un délai raisonnable, d'un commun accord entre les PARTIES.

4. Notification en cas d'illégalité : ATOSS informera immédiatement le CLIENT si ATOSS estime que les instructions données par le CLIENT sont contraires au RGPD ou aux dispositions de l'Union ou des États membres applicables en matière de protection des données. Cette obligation d'information n'implique pas un examen juridique complet. ATOSS est en droit de suspendre l'exécution de l'instruction jusqu'à ce qu'elle soit confirmée ou modifiée par le CLIENT.

5. Droits des personnes concernées : ATOSS ne peut pas fournir des informations aux personnes concernées par le traitement des données ou à des TIERS qu'après avoir reçu des instructions préalables du CLIENT. Si une personne concernée s'adresse directement à ATOSS à ce sujet, ATOSS transmettra immédiatement cette demande au CLIENT.

6. Recours : Si ATOSS devait être exposé à une responsabilité justifiée suite à la mise en œuvre d'une instruction illégale, ATOSS peut se faire indemniser par le CLIENT.

**§ 5 Engagement de confidentialité**

1. Secret des données et des télécommunications : ATOSS et toute personne sous l'autorité d'ATOSS ayant accès aux données à caractère personnel traitées sont tenus à la confidentialité, notamment conformément aux dispositions de l'art. 5, par. 1, point f), art. 28, par. 3 point b), art. 29 et art. 32, par. 4, du RGPD ainsi que de l'art. 3 de la TDDDG [Telekommunikation-Telemedien-Datenschutz-Gesetz - loi allemande sur la

protection des données dans le domaine des télécommunications et des télémédias]. L'obligation de confidentialité se poursuit même après la fin du présent CTD.

2. Instruction de toutes les personnes chargées du traitement des données à caractère personnel : ATOSS s'assure, par des mesures appropriées telles que notamment des formations régulières sur la protection des données, que les personnes placées sous son autorité et autorisées à traiter des données à caractère personnel connaissent les dispositions applicables en matière de confidentialité des données et de secret des télécommunications.

**§ 6 Recours à des sous-traitants**

1. [Reste libre pour des raisons éditoriales]

2. Conditions d'admissibilité du recours : Le recours à des sous-traitants n'est possible qu'avec l'accord du CLIENT.

a) Exigences générales : Lorsque ATOSS charge un sous-traitant d'exécuter certaines activités de traitement (pour le compte du CLIENT), cette sous-traitance s'effectue par un contrat qui impose au sous-traitant essentiellement les mêmes obligations en matière de protection des données que celles qui s'appliquent à ATOSS en vertu du présent CTD. ATOSS s'assure que le sous-traitant remplit les obligations auxquelles ATOSS est soumis conformément au présent CTD et au RGPD. ATOSS fournira au CLIENT, à sa demande, une copie d'un tel accord de sous-traitance et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire à la protection des secrets commerciaux ou d'autres informations confidentielles, y compris les données à caractère personnel, ATOSS peut masquer le texte de l'accord avant d'en transmettre une copie.

   ATOSS est pleinement responsable envers le CLIENT de l'exécution par le sous-traitant de ses obligations en vertu du CONTRAT conclu avec ATOSS. ATOSS informera le CLIENT si le sous-traitant ne respecte pas ses obligations contractuelles en ce qui concerne les services fournis au CLIENT.

b) Sous-traitants dans des pays tiers : Tout transfert de données par ATOSS vers un pays tiers ou une organisation internationale se fait exclusivement sur la base des instructions documentées du CLIENT (cf. art. 4) ou pour respecter une disposition spécifique en vertu du droit de l'Union ou du droit d'un État membre auquel ATOSS est soumis, et doit être conforme au chapitre V du RGPD.

   Dans les cas où ATOSS fait appel à un sous-traitant conformément au présent art. 6 pour l'exécution de certaines activités de traitement (pour le compte du CLIENT) et où ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du RGPD, ATOSS et son sous-traitant peuvent assurer le respect du chapitre V du RGPD en utilisant des clauses contractuelles types approuvées par la Commission conformément à l'art. 46, par. 2, du RGPD, pour autant que les conditions d'application de ces clauses contractuelles types soient remplies.

3. Sous-traitants actuels : ATOSS dispose de l'autorisation générale du CLIENT pour recourir à des sous-traitants dont la liste figure à **l' CTD-Annexe III - Liste des sous-traitants autorisés à** ce CTD. En ce qui concerne le recours à ces sous-traitants, le consentement du CLIENT est réputé acquis à la conclusion du présent CTD.

4. Autres sous-traitants : La poursuite de l'externalisation vers des sous-traitants ou le changement de sous-traitants existants sont autorisés dans les conditions de l'art. 6 point 2 du présent CTD, même sans le consentement exprès du CLIENT, dans la mesure où ATOSS informe le CLIENT de l'externalisation vers des (autres) sous-traitants un délai raisonnable à l'avance (par exemple par e-mail ou via un portail en ligne accessible via le site Internet d'ATOSS) et que les dispositions suivantes sont respectées : ATOSS informera le CLIENT au moins 6 semaines à l'avance de toute modification prévue de cette liste, en incluant ou en remplaçant des sous-traitants et donnera ainsi au CLIENT suffisamment de temps pour s'opposer à ces modifications avant de faire appel au(x) sous-traitant(s) concerné(s).

   ATOSS fournira au CLIENT une liste mise à jour de tous les sous-traitants qui ont accès aux données à caractère personnel du CLIENT, ainsi que les services limités ou complémentaires qu'ils fournissent. En notifiant ces modifications, ATOSS donne au CLIENT la possibilité de s'y opposer dans un délai de six (6) semaines. Le CLIENT n'a le droit de s'y opposer que si les modifications ne répondent pas aux exigences de l'art. 6 point 2 du présent CTD. Si le CLIENT ne s'oppose pas ou ne s'oppose pas de manière justifiée aux modifications par écrit dans le délai d'opposition, l'accord aux modifications est considéré comme donné après l'expiration du délai. En cas d'opposition justifiée, ATOSS peut suspendre l'intervention du sous-traitant modifié concerné par l'opposition justifiée du CLIENT. Dans le cas où le CLIENT s'oppose à l'utilisation, même après avoir consulté ATOSS, ce dernier peut choisir de ne pas faire appel au sous-traitant ou de résilier le CONTRAT par écrit avec un préavis de deux (2) mois. Cette disposition complète les règles de résiliation du CONTRAT.

5. Application des dispositions du présent CTD également aux sous-traitants : À la demande du CLIENT, ATOSS fournira au CLIENT des informations sur les obligations du sous-traitant en matière de protection des données, y compris, mais sans s'y limiter, la fourniture de l'accès nécessaire aux documents contractuels pertinents. ATOSS contrôlera régulièrement ses sous-traitants et confirmera, à la demande du CLIENT, le respect de la législation sur la protection des données et des obligations du sous-traitant en vertu du contrat de traitement des données conclu avec lui. Ce n'est qu'en présence de motifs légitimes que le CLIENT est en droit de donner des instructions à ATOSS pour qu'il procède à des contrôles supplémentaires, qu'ATOSS effectuera dans la limite de ce qui est autorisé.

**§ 7 Obligations et droits du CLIENT ; assistance du CLIENT par ATOSS**

Le CLIENT est tenu de respecter les droits de la personne concernée (art. 12 et ss.du RGPD ), de prendre les mesures techniques et organisationnelles, de notifier et d'informer en cas de violation de la protection des données, de coopérer avec l'autorité de contrôle (art. 32 à 36 du RGPD) ainsi que de garantir la qualité (art. 28, par. 1, du RGPD). ATOSS assiste le CLIENT dans le respect de ses obligations. Dans ce contexte, ATOSS lui fournit toutes les informations dans la mesure où le CLIENT n'en dispose pas lui-même. ATOSS n'est pas tenu de fournir des informations à des fins d'assistance dont ATOSS ne dispose pas de son côté. ATOSS assiste le CLIENT de la manière suivante :

1. Respect des droits des personnes concernées : ATOSS informe immédiatement le CLIENT de toute demande reçue d'une personne concernée du CLIENT. ATOSS ne répond pas lui-même à la demande. Il incombe au CLIENT de préserver les droits des

Personnes concernées. Si nécessaire, ATOSS assiste le CLIENT en cas d'exercice des droits par les Personnes concernées.

2. Mesures techniques et organisationnelles : ATOSS assiste le CLIENT pour assurer un niveau de protection adéquat en prenant des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement ainsi que de la probabilité et de la gravité prévues d'une éventuelle violation de la sécurité et qui permettent de détecter en temps utile les événements de violation pertinents. Le CLIENT doit notamment s'assurer que les PRODUITS ATOSS mis à disposition par ATOSS ainsi que les interfaces techniques y afférentes sont protégés contre tout accès non autorisé (par ex., par l'attribution d'identifiants d'accès uniquement valables temporairement et/ou par des modifications régulières du mot de passe et/ou par des restrictions de la plage d'adresses IP autorisées à l'accès ou par d'autres mesures comparables) sous une forme appropriée et adaptée au besoin de protection.

3. Obligation de déclaration et de notification : En cas de violation de la protection des données à caractère personnel par ATOSS, ce dernier est tenu d'assister le CLIENT en ce qui concerne son obligation de notification à l'autorité de contrôle compétente et son obligation de notification aux Personnes concernées. En cas de perturbation grave de l'exploitation, de suspicion de violation de la protection des données ou de violation du présent CTD, qu'elle soit le fait du CLIENT, d'un tiers ou d'ATOSS, ATOSS doit informer le CLIENT sans délai et de manière complète de la date, du type et de l'étendue des données à caractère personnel concernées. Toutes les informations pertinentes pour satisfaire à l'obligation de notification à l'autorité de contrôle doivent être mises à la disposition du CLIENT sans délai. Si toutes ces informations ne peuvent être fournies simultanément, la notification initiale contiendra les informations disponibles à ce moment-là et les informations complémentaires seront fournies ultérieurement, dès qu'elles seront disponibles, sans retard injustifié.

4. Coopération avec l'autorité de contrôle : Les PARTIES coopèrent avec l'autorité de contrôle compétente dans l'accomplissement de leurs tâches, dans la mesure nécessaire, conformément aux principes suivants.

a) Activités de contrôle chez ATOSS ou chez le CLIENT :

(aa) ATOSS informera immédiatement le CLIENT des actes de contrôle et des mesures prises par l'autorité de contrôle, dans la mesure où ils se rapportent au CONTRAT. Il en va de même dans la mesure où une autorité compétente enquête, dans le cadre d'une procédure d'infraction ou pénale, sur le traitement de données à caractère personnel effectué dans le cadre du traitement des données chez ATOSS.

(bb) Dans la mesure où le CLIENT est à son tour exposé à un contrôle de l'autorité de surveillance, à une procédure d'infraction ou pénale, à une action en responsabilité d'une personne concernée ou d'un tiers ou à toute autre action en relation avec le traitement des données auprès d'ATOSS, ATOSS doit lui apporter son soutien dans la mesure de ses possibilités.

b) Évaluation de l'impact sur la protection des données : Dans la mesure où le CLIENT est légalement tenu de réaliser une analyse d'impact relative à la protection des données, ATOSS l'aidera à réaliser cette analyse et à consulter préalablement l'autorité de contrôle, le cas échéant, dans la mesure nécessaire. Cela comprend notamment

le transfert des données éventuellement nécessaires ou la divulgation des documents éventuellement nécessaires à la demande du CLIENT.

5. Documentation et conformité :

a) Examens : Les Parties doivent pouvoir démontrer la conformité avec les présentes Clauses. ATOSS traitera rapidement et de manière appropriée les demandes du CLIENT concernant le traitement des données conformément au présent CTD. ATOSS met à la disposition du CLIENT toutes les informations nécessaires à la preuve du respect des obligations définies dans le présent CTD et découlant directement du RGPD. À la demande du CLIENT, ATOSS autorise également et contribue à l'audit des activités de traitement couvertes par le présent CTD à des intervalles raisonnables ou en cas d'indices de non-conformité. Pour décider d'un audit, le CLIENT peut prendre en compte les informations et les certifications pertinentes d'ATOSS.

Le CLIENT peut effectuer lui-même à l'audit ou faire appel à un auditeur indépendant ATOSS peut s'opposer à l'examen par un auditeur indépendant si celui choisi par le CLIENT est dans une relation de concurrence avec ATOSS ou n'a pas été engagé à respecter la confidentialité.

Les coûts des contrôles selon l'art. 7 (5) point a) sont à la charge du CLIENT.

b) Documentation : La preuve de la documentation des mesures techniques et organisationnelles peut notamment être apportée par le respect de codes de conduite approuvés conformément à l'art. 40 du RGPD ou par une preuve appropriée d'un audit de sécurité informatique ou de protection des données.

c) Délégué à la protection des données : Les coordonnées du délégué à la protection des données sont mentionnées dans l' **CTD-Annexe II - Mesures techniques et organisationnelles**.

**§ 8 Effacement ou restitution à la fin du traitement**

1. Suppression ou restitution : L'effacement et la restitution des données à caractère personnel sont régis par les dispositions du **CTD-Annexe I - Description du traitement** et par les dispositions contractuelles.

2. [Reste libre pour des raisons éditoriales]

3. Délais de conservation : Les documents qui servent à prouver le traitement des données conformément à la commande et à la réglementation doivent être conservés par ATOSS conformément aux délais de conservation légaux respectifs au-delà de la fin du présent CTD. ATOSS peut les remettre au CLIENT à sa décharge après la fin du présent CTD.

4. Coûts : Les frais supplémentaires occasionnés par des instructions du CLIENT dérogeant au présent art. 8 point 1 ou allant au-delà de celui-ci sont à la charge du CLIENT.

## § 9 Responsabilité et droit à indemnisation

1. Les parties sont responsables au titre du présent CTD conformément aux dispositions légales du RGPD.

2 [reste libre pour des raisons rédactionnelles].

3) [reste libre pour des raisons rédactionnelles]..

## § 10 Dispositions finales

1. Clause de remplacement ; modifications et ajouts :

a) Le présent CTD entre en vigueur à la conclusion du CONTRAT et remplace, dès son entrée en vigueur, dans son domaine d'application, tous les accords de traitement des données éventuellement existants entre les PARTIES.

b) Sauf disposition contraire expresse, les modifications et compléments apportés au présent CTD ainsi que toutes les conventions annexes requièrent la forme écrite pour être valables.

c) Sans préjudice des dispositions de l'art. 3, point 3 (état actuel de la technique et adaptations techniques) et de l'art. 6 point 4 (autres sous-traitants), ATOSS est en droit de modifier ou de compléter les dispositions du présent CTD, dans la mesure où cela n'affecte pas négativement le rapport d'équivalence convenu lors de la conclusion du contrat en ce qui concerne les éléments essentiels du contrat et que les modifications sont acceptables pour le CLIENT. Le pouvoir d'adaptation s'étend ici en particulier aux modifications relatives (i) aux développements techniques, (ii) aux modifications du cadre juridique, (iii) à la suppression d'une perturbation de l'équivalence survenue ultérieurement ou (iv) à la suppression de lacunes réglementaires (par exemple en cas de circonstances imprévisibles et changeantes). ATOSS informera préalablement le CLIENT des modifications prévues. Les modifications seront considérées comme acceptées par le CLIENT s'il ne les conteste pas par écrit dans un délai de six (6) semaines suivant la notification de la modification à ATOSS. Dans l'avis de modification, ATOSS attire également l'attention du CLIENT sur la signification prévue de son comportement.

2. Non-application des conditions générales de vente / d'achat du CLIENT : Il est convenu entre les PARTIES que les « conditions générales de vente » et / ou les « conditions générales d'achat » du CLIENT ne s'appliquent pas au présent CTD.

3. Exclusion du droit de rétention : L'exception du droit de rétention est exclue en ce qui concerne les données à caractère personnel traitées et les supports de données correspondants.

4. [Reste libre pour des raisons éditoriales]

5. Obligation d'informer en cas de risque pour les données à caractère personnel : Dans le cas où les données à caractère personnel chez ATOSS seraient menacées par une saisie ou une confiscation, par une procédure d'insolvabilité ou de règlement judiciaire ou par tout autre événement ou mesure prise par un tiers, ATOSS est tenu d'en informer immédiatement le CLIENT.

6. Juridiction compétente : Les dispositions de l'art. 10, point 7, du présent CTD sont applicables.

7. Voies de recours : Les recours d'une Personne concernée contre ATOSS en tant que sous-traitant sont régis par les dispositions applicables en matière de protection des données. Les recours des PARTIES découlant du présent CTD ou en rapport avec celui-ci sont régis par les dispositions du CONTRAT en ce qui concerne le choix de la loi applicable et le lieu de juridiction.
8. Clause de sauvegarde : Si certaines parties du présent CTD sont ou deviennent totalement ou partiellement invalides ou inapplicables, la validité des autres dispositions n'en est pas affectée. Les PARTIES s'engagent à convenir, en lieu et place de la disposition invalide ou inapplicable, d'une disposition valable et applicable qui se rapproche le plus possible du sens et de l'objectif initialement voulus par la disposition invalide ou inapplicable. Il en va de même en cas de lacune réglementaire.

**CTD-Annexe I**

- Description du traitement -

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

   En fonction du CLIENT, les personnes suivantes peuvent être concernées par le traitement :

   - Employés au sens de l'art. 26, al. 8 BDSG [Bundesdatenschutzgesetz - Loi allemande sur la protection des données]
   - Fonctionnaires ainsi que candidats et candidates des Länder
   - Salariés sous convention collective et en formation professionnelle

2. **Catégories de données à caractère personnel traitées :**

   Les catégories de données à caractère personnel effectivement traitées dans le cadre de chaque CONTRAT dépendent essentiellement de la configuration et des paramètres choisis par le CLIENT ainsi que de la sélection des modules convenue.

   Des informations complémentaires peuvent être tirées des documents contractuels et/ou d'autres informations mises à disposition (par ex. dans le cadre de l'utilisation de notre site Internet, salon numérique pour les clients).

   Les catégories de données à caractère personnel pertinentes peuvent notamment être les suivantes :

a) **Données de base des salariés et informations sur la gestion des temps**

   - Données de base, comme :
     - Matricule
     - Titre, nom, prénom
     - Date de naissance
     - Numéro(s) de carte(s) d'identité
     - Catégorie d'employés (par ex., affectation au modèle de facturation)
     - Autres données relatives au contrat, telles que les données d'entrée, de sortie et de reclassement
     - Accords sur le temps de travail ainsi que sur le début et la fin de la prise en compte de la gestion du temps de travail
     - Coordonnées (telles que l'adresse, l'e-mail, les numéros de téléphone)
     - Photo du personnel
     - Autres caractéristiques organisationnelles
   - Informations sur l'appartenance à certaines régions, pays, langues
   - Informations sur les lieux de travail et les temps de trajet
   - Informations sur les relations avec les supérieurs, les collaborateurs et les suppléants
   - Autres données à caractère personnel enregistrées par les utilisateurs finaux dans des champs librement définissables
   - Informations sur les qualifications et les formations
   - Informations sur les soldes et les comptes horaires

- Informations sur les droits des salariés en matière de rémunération, de congés et de temps libre, conformément aux contrats individuels, aux conventions collectives et autres:
    - Accords généraux
    - Valeurs et soldes
- Informations sur les absences prévues et effectives
- Informations sur les réservations ou les pointages, y compris l'heure et le lieu de la réservation ou du pointage
- Informations sur les heures de présence, de disponibilité (d'appel) et de travail effectives
- Informations sur l'appartenance à des unités d'organisation, projets, missions, centres de coûts, postes de travail, etc. et sur le temps passé à les réaliser
- Réservations de cantine
- Annotations manuelles des données de base et altérables
- Avertissements et messages d'erreur côté système en cas d'écarts par rapport aux directives ou aux règles

**b) Informations de la planification des ressources humaines**

- Informations sur la disponibilité contractuelle et planifiée du personnel
- Informations sur les souhaits de planification des salariés
- Informations sur les plannings des employés et les heures de travail réellement effectuées
- Informations sur les changements de plans
- Informations sur les opérations de changement d'équipe des salariés
- Informations sur les profils de performance des employés

**c) Gestion des demandes et des tâches**

- Demandes d'absences, y compris le déroulement et le statut de l'approbation
- Demandes pour des opérations liées au temps de travail ou à l'organisation du service, y compris le déroulement et le statut de l'approbation
- Tâches en attente et accomplies
- Informations sur les notifications par e-mail et SMS envoyées par le système

**d) Informations de la gestion des accès**

- Informations sur les autorisations d'accès pour des appareils, zones et périodes spécifiques
- Identifiants d'accès
- Code PIN à saisir sur l'appareil
- Caractéristiques d'identification pour la sécurité d'accès biométrique (procédé d'empreintes digitales, etc.)
- Informations sur les entrées ou sorties de zones effectives ou tentées, y compris l'heure et le lieu de la réservation

**e) Informations relatives au système**

- Informations sur l'accès au système
- Informations sur les autorisations pour certains objets et interactions en tant qu'utilisateur du système
- Protocole Internet (IP), informations sur les paquets, y compris les URL, l'horodatage, les données télémétriques, les ports relatifs à l'utilisation des services de cloud ATOSS

- Informations sur le navigateur (agents utilisateurs du navigateur, données de log) en rapport avec l'utilisation d'ATOSS Cloud Services
- Paramètres système et préférences récemment utilisés
- Utilisateurs système connectés
- Tentatives de connexion
- Journaux des interactions avec les utilisateurs qui modifient les données dans le système.

**f) Données sensibles**

Lorsque le transfert concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives à des condamnations pénales et à des infractions (ci-après les «données sensibles»), ATOSS applique des restrictions particulières et/ou des garanties supplémentaires.

**3. Type de traitement**

**a) Activités de traitement**

Les services d'ATOSS peuvent comprendre - comme décrit plus en détail dans le contrat respectif avec le CLIENT - notamment les activités de traitement suivantes :

- Customizing [personnalisation] au sens du paramétrage des PRODUITS ATOSS (en particulier, assistance à la création des données de base des employés dans la base de données du logiciel standard mis à disposition du CLIENT par ATOSS pour l'utilisation, à la mise en place de modèles de temps de travail et de comptes horaires, etc.) et adaptation ou scriptage d'interfaces standard ;
- Maintenance des logiciels concernant les PRODUITS ATOSS (en particulier, assistance lors des changements de versions des logiciels, de l'installation de modifications continues ainsi que de la correction des dysfonctionnements signalés) ;
- Prestations de hotline concernant les PRODUITS ATOSS (notamment la réception d'informations ou l'aide à l'analyse pour les dysfonctionnements signalés ; dépannage lors du transfert de données par interface vers des systèmes tiers (par ex. paie et salaire) ainsi que lors de la saisie de données avec des terminaux de saisie) ;
- Travaux de contrôle et de maintenance de procédures automatisées ou d'installations de traitement de données pour assurer la disponibilité opérationnelle des PRODUITS ATOSS.
- Prestations de services gérés relatifs à l'administration des données à caractère personnel, conformément à la portée définie dans le CONTRAT (notamment une assistance active pour l'administration des données à caractère personnel des employés du CLIENT dans le PRODUIT ATOSS fourni par ATOSS)

Les activités de traitement - qu'elles soient totales ou partielles - peuvent alors avoir lieu :

- Sur le site du CLIENT (au choix du CLIENT, en accédant directement à ses systèmes informatiques ou en établissant une connexion entre un ordinateur client d'ATOSS et les systèmes informatiques du CLIENT) ;
- Par accès à distance via une connexion VPN sécurisée et une solution logicielle d'accès à distance fournie par le CLIENT (par ex. VPN, partage de bureau) qui fonctionne sur les systèmes d'exploitation Windows Server actuels (y compris la licence nécessaire) ou,

dans le cas des PRODUITS ATOSS, par accès à distance via une connexion VPN sécurisée aux systèmes informatiques de l'exploitant des infrastructures Cloud sur lesquelles les données à caractère personnel du CLIENT sont traitées.

Dans tous les cas, un accès en lecture et en écriture à la base de données intégrée dans les PRODUITS ATOSS et, le cas échéant, aux autres systèmes de traitement de l'information qui y sont liés chez le CLIENT et qui contiennent des données à caractère personnel, ne peut être exclu.

**b) Limitation matérielle du traitement**

ATOSS n'est pas autorisé à traiter les données à caractère personnel du client au-delà de ce qui est prévu par le présent CTD. Le traitement à d'autres fins, notamment la transmission arbitraire de données à des TIERS, n'est pas autorisé. ATOSS est tenu de traiter séparément les données à caractère personnel de différents clients.

**c) Limitation locale**

La fourniture des services de traitement des données convenus dans le cadre d'un CONTRAT a lieu en principe dans un État membre de l'Union européenne (UE) ou dans un autre État partie à l'accord sur l'Espace économique européen (EEE) ou en Suisse (CH).

Si le traitement des données a lieu dans un pays tiers, c'est-à-dire en dehors de l'UE, de l'EEE ou de la Suisse, ATOSS s'assure que les conditions particulières de l'art. 44 et suivants du RGPD ainsi que les dispositions du présent CTD sont remplies.

**d) Journalisation des opérations de traitement**

Les PARTIES s'engagent à n'accéder à la base de données intégrée dans les PRODUITS ATOSS et aux données à caractère personnel qui y sont traitées qu'en utilisant des identifiants distincts. Cela suppose que le CLIENT attribue à ATOSS des identifiants d'utilisateur séparés à utiliser dans le cadre du traitement des données et qu'il participe à leur mise en place dans la mesure nécessaire. ATOSS rendra ces identifiants accessibles exclusivement au personnel nécessaire à l'exécution des prestations et les protégera par des mesures appropriées et raisonnables contre toute consultation ou utilisation non autorisée.

**4. Finalité(s) du traitement**

ATOSS ne traitera les données à caractère personnel du CLIENT qu'aux fins spécifiques mentionnées dans le CONTRAT, sauf instructions contraires données par le CLIENT à ATOSS. La finalité fondamentale du traitement est de garantir la fonctionnalité et l'actualité des PRODUITS ATOSS mis à la disposition du CLIENT par ATOSS pour utilisation.

**5. Durée du traitement**

Les données à caractère personnel fournies par le CLIENT seront traitées par ATOSS pour la durée indiquée dans le CONTRAT entre les PARTIES. Celle-ci correspond généralement à la durée du CONTRAT, y compris les éventuelles obligations post-contractuelles. Si la durée du contrat n'est pas précisée, la durée du traitement des données à caractère personnel commence au début des prestations dues et se termine à la fin des obligations en cas de résiliation du contrat. L'obligation d'effacement ne s'applique pas si le droit de l'Union ou le droit national applicable impose une obligation de conserver les données, notamment en vertu de la législation fiscale ou du bilan commercial.

***

**CTD-Annexe II**

- Mesures techniques et organisationnelles -

Toutes les succursales et les sociétés du groupe ATOSS Software SE utilisent l'ensemble de l'infrastructure informatique du siège de l'entreprise à Munich. Toutes les activités - même à distance - sont réalisées exclusivement avec des ressources informatiques et des moyens d'exploitation mis à disposition par ATOSS Software SE et contrôlés de manière centralisée. Le centre de données interne se trouve à Munich.

Les mesures techniques et organisationnelles prises par ATOSS en ce qui concerne les systèmes informatiques internes et les processus commerciaux internes des succursales et des sociétés du groupe ATOSS Software SE sont présentées ci-dessous. Des différences (minimes) sont possibles en fonction du site ATOSS.

## I. CONFIDENTIALITE

### 1. Contrôle d'accès physique

Mesures susceptibles d'empêcher les personnes non autorisées d'accéder aux bureaux, postes de travail et installations internes de traitement des données.

| | | |
|---|---|---|
| **I.1.1** | **Bureaux et lieux de travail** | |
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒Système d'alarme anti-intrusion (EMA)<br>☒ Système de fermeture électronique<br>☒ Techniques d'accès (par ex., RFID, PIN ou clés mécaniques) avec attribution spécifique aux personnes<br>☒Système de fermeture mécanique pour le bâtiment / les bureaux<br>☒ Cartes à puce<br>☒ Sonnerie avec caméra<br>☒ Vidéosurveillance des zones d'entrée<br>☒ Détecteur de mouvement, détecteur d'agression<br>☒Service de garde | ☒ Responsable de site<br>☒ La sortie des clés est consignée au moyen de protocoles de sortie et de retour<br>☒ Zones de sécurité<br>☒ Zones d'accueil/de visite<br>☒ Limitation de l'accès aux personnes étrangères à l'entreprise (p. ex. visiteurs)<br>☒ Processus de gestion des visiteurs, y compris (dé)enregistrement, badges visiteurs, accompagnement par des collaborateurs<br>☒ Rigueur dans le choix du service de garde |
| **I.1.2** | **Centre de données interne** | |
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Exploitation du centre de données interne par le service informatique d'ATOSS<br>☒Système d'alarme anti-intrusion (EMA)<br>☒ Système de fermeture électronique<br>☒ Technique d'accès (par ex. RFID et clés mécaniques) avec attribution spécifique aux personnes<br>☒ Vidéosurveillance | ☒ Limitation de la remise des clés et restriction des droits d'accès au centre de calcul au personnel privilégié du service informatique d'ATOSS<br>☒ La sortie des clés est consignée au moyen de protocoles de sortie et de retour<br>☒ Processus de gestion des visiteurs, y compris (dé)enregistrement, badges visiteurs, accompagnement par des collaborateurs |

**2. Contrôle d'accès numérique**

Mesures propres à empêcher que les installations internes de traitement des données et les informations puissent être utilisées par des personnes non autorisées.

| I.2 | **Systèmes internes, applications, ordinateurs portables, smartphones** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Connexion des succursales et des sociétés du groupe par réseau de serveurs cryptés (contrôleur de domaine)<br>☒ Utilisation uniquement de l'équipement informatique et des applications, systèmes approuvés en interne par ATOSS<br>☒ Interdiction du BYOD [PAP]<br>☒ Authentification des disques durs basée sur le BIOS des terminaux mobiles (par ex., ordinateurs portables, tablettes)<br>☒ Verrouillage du boîtier<br>☒ Connexion avec des comptes d'utilisateurs personnalisés + mot de passe<br>☒ Connexion avec des comptes privilégiés + mot de passe + 2. Facteur<br>☒ Enregistrement des inscriptions et des désinscriptions, tentatives d'inscription<br>☒ Verrouillage automatique du bureau / de l'écran protégé par mot de passe<br>☒ Interdiction avec réserve d'exception pour l'utilisation de supports amovibles à cryptage matériel (p. ex. clés USB avec AES 256 bits)<br>☒ Utilisation de la connexion VPN en cas d'accès à distance<br>☒ Gestion des appareils mobiles<br>☒ Cryptage des disques durs (AES 256 bits)<br>☒ Protection contre les virus, les logiciels espions et malveillants<br>☒ SIEM [GIES]<br>☒ Pare-feu<br>☒ Filtre anti-spam<br>☒ Web Proxy (y compris protection antivirus)<br>☒ Système de détection/prévention d'intrusion (IDS/IPS)<br>☒ Serveur de mots de passe<br>☒ Cryptage du transfert de données (par ex., mots de passe BIOS, connexions VPN, cryptshare, Ironkeys y compris scanner de virus)<br>☒ Les applications sont examinées pour déterminer s'il est techniquement possible d'empêcher ou de fermer les interfaces. | ☒ Gestion des utilisateurs et des autorisations<br>☒ Gestion des mots de passe<br>☒ Limitation des tentatives de connexion et blocage automatique de l'accès<br>☒ Directive sur l'utilisation des mots de passe et la protection des accès<br>☒ Valeurs par défaut pour le blocage manuel<br>☒ Historique des mots de passe<br>☒ Directive sur le traitement des valeurs de l'entreprise, y compris effacement/destruction<br>☒ Directive sur la protection des données et la sécurité de l'information dans l'organisation<br>☒ Directive Smartphones<br>☒ Directive Médias Sociaux<br>☒ Contrôle et conservation des procès-verbaux<br>☒ Mises à jour de sécurité<br>☒ Analyse des points faibles (mensuelle)<br>☒ Tests d'intrusion (annuels)<br>☒ Gestion des incidents<br>☒ Gestion du changement<br>☒ Gestion des urgences informatiques |

### 3. Contrôle d'accès

Mesures garantissant que les personnes autorisées à utiliser les systèmes internes de traitement des données ne peuvent accéder qu'aux informations relevant de leurs droits d'accès et que les informations ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation pendant le traitement, l'utilisation et après le stockage.

| I.3 | **Informations (qu'elles soient sous forme électronique ou physique)** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Les droits d'accès sont définis, coordonnés et contrôlés par un Microsoft Active Directory central ou un domaine propre à l'entreprise.<br>☒ Journalisation des accès aux applications (saisie, modification et suppression des droits d'accès)<br>☒ Coffre-fort de protection des données<br>☒ Casiers d'employés<br>☒ Destruction des supports de données électroniques par un prestataire de services d'élimination externe (norme DIN 66399-3)<br>☒ Élimination des documents classifiés dans des conteneurs de données scellés<br>☒ Destruction des documents et vidage par un prestataire de services d'élimination externe | ☒ Concept d'autorisation basé sur les rôles<br>☒ Gestion des utilisateurs et des autorisations (y compris les directives en cas d'entrée, de changement de fonction, de départ)<br>☒ Nombre limité d'administrateurs / de comptes d'utilisateurs privilégiés<br>☒ Directive sur le traitement des valeurs de l'entreprise, y compris effacement/destruction<br>☒ Directive Clean Desk<br>☒ La distribution des clés de casiers est consignée dans des protocoles de distribution et de restitution.<br>☒ Contrôle et conservation des procès-verbaux<br>☒ Rigueur dans le choix du prestataire de services d'élimination des déchets<br>☒ Points d'accès distincts pour les systèmes informatiques externes |

### 4. Contrôle de séparation

Mesures garantissant que les données collectées à des fins différentes sont traitées séparément, logiquement ou physiquement.

| I.4 | **Contrôle du système / de la mémoire** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Séparation des données à caractère personnel du CLIENT dans le cadre d'un traitement des données de commande et des autres informations commerciales internes<br>☒ Séparation des systèmes de production et de test<br>☒ Multi-localisation des applications pertinentes<br>☒ Les tests de logiciels / matériels sont effectués dans des environnements virtuels isolés (Sandboxing) | ☒ Interdiction de transmettre des données à caractère personnel du CLIENT dans le sens d'un traitement des données de commande en dehors des voies de transfert et de communication définies, à ATOSS<br>☒ Définition des droits internes de la base de données<br>☒ Gestion interne du domaine<br>☒ Plans de topologie du réseau interne<br>☒ Gestion du changement |

## II. INTEGRITE

### 1. Contrôle de saisie

Mesures garantissant qu'il est possible de vérifier et déterminer a posteriori si, et par qui, des informations ont été saisies, rectifiées ou effacées dans des systèmes internes de traitement des données.

| II.1 | **Enregistrement / Journalisation (par ex., systèmes d'exploitation, réseaux, pares-feux, bases de données, applications)** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Journalisation technique des connexions et déconnexions des utilisateurs sur les systèmes de traitement de données internes ATOSS<br>☒Stockage centralisé des données de journalisation relatives aux systèmes de traitement de données internes ATOSS<br>☒ Synchronisation de l'horloge/serveur de temps | ☒ Les restrictions de saisie, de modification et de suppression basées sur les rôles sont contrôlées et gérées par la gestion des utilisateurs et des autorisations.<br>☒ Conservation des procès-verbaux conformément aux exigences légales<br>☒ Contrôle manuel ou automatisé des procès-verbaux |

### 2. Contrôle du transfert

Mesures garantissant que les données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation lors de leur transfert électronique ou pendant leur transport ou leur stockage sur des supports de données, et qu'il est possible de vérifier ou déterminer à quels organismes un transfert de données à caractère personnel par des installations de transfert de données est destinée.

| II.2 | **Transferts de données électroniques et physiques** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Cryptage des e-mails (S/MIME, TLS, certificats)<br>☒ Filtre de contenu pour la messagerie et le Web<br>☒ Cryptage de la téléphonie (SAML, TLS, certificats)<br>☒ Utilisation du VPN sur les terminaux mobiles<br>☒ Interdiction avec réserve d'autorisation spéciale pour l'utilisation de supports amovibles à cryptage matériel (p. ex. clés USB avec AES 256 bits)<br>☒ Boîtes aux lettres fermées à clé<br>☒ Utilisation de voies de communication et de transfert définies | ☒ Directive sur les transferts d'informations de et vers l'extérieur<br>☒ Retrait du courrier uniquement par le personnel de réception de l'entreprise<br>☒ Distribution personnelle pour le courrier externe<br>☒ Distribution personnelle en cas de courrier/documents internes marqués (très) confidentiels<br>☒ Livraisons de marchandises uniquement dans les zones de livraison avec réception personnelle<br>☒ Préférences définies en cas d'accès à distance (voir informations complémentaires ci-dessous*)<br>☒ Prévention / suppression des transferts de données à caractère personnel non anonymisées du CLIENT en dehors des voies de transfert coordonnées et définies (voir informations complémentaires*) |

***Informations complémentaires :**

Le transfert de données à caractère personnel non anonymisées du CLIENT ne peut être effectuée que par le CLIENT lui-même, soit par les voies de transfert mises en place dans les Services ATOSS Cloud, soit sur les systèmes informatiques propres au client. L'envoi de données à caractère personnel non anonymisées du CLIENT par courrier électronique à des destinataires chez ATOSS est à proscrire.

Pour la fourniture de prestations de paramétrage, de maintenance de logiciels et de hotline avec accès à l'installation client sous licence, le CLIENT doit assurer le contrôle d'accès et de transfert par des configurations appropriées dans la gestion des utilisateurs :

- L'enregistrement ou le désenregistrement des utilisateurs (y compris des conseillers de la hotline et Customer Service [Assistance Clientèle] ATOSS) ne peut être effectué que par le CLIENT et contrôlé selon des cycles de contrôle qu'il a spécialement définis.
- Les prestations de paramétrage, de maintenance logicielle et de hotline avec accès à l'installation client sous licence sur les systèmes informatiques du CLIENT sur place ou à distance nécessitent une autorisation d'utilisation ou une activation préalable par le CLIENT.
- Les prestations de paramétrage, de maintenance logicielle et de hotline à distance s'effectuent exclusivement via des connexions sécurisées et dans le respect des mesures techniques et organisationnelles de protection des données à caractère personnel décrites dans la présente annexe.
- Dans la mesure où cela est nécessaire, les conseillers Hotline et Customer Service ATOSS participent, sur instruction du CLIENT, à la configuration des dispositifs techniques de contrôle. Dans la mesure où des accès à distance doivent être effectués sur les systèmes informatiques du client, le CLIENT met à disposition une solution logicielle appropriée pour l'accès à distance (par ex. VPN, Desktop Sharing), qui fonctionne sur les systèmes d'exploitation Windows Server actuels (y compris la licence nécessaire). Les accès à distance sont contrôlés et gérés par le département ATOSS Remote Access Services (RAS).
- Le CLIENT est habilité à suivre les accès à distance et à les interrompre à tout moment.
- Les données à caractère personnel du CLIENT ne peuvent être stockées sur des supports de données amovibles d'ATOSS que sur instruction expresse du CLIENT. Les copies correspondantes sont supprimées par ATOSS à la fin de l'accès concret.

## III. DISPONIBILITE

Mesures garantissant que les données à caractère personnel sont protégées contre la destruction ou la perte accidentelles.

| I.1.1 | **Bureaux et postes de travail, matériel, ressources informatiques** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Dispositifs de protection contre l'incendie (par ex., systèmes de détection d'incendie et de fumée)<br>☒ Portes coupe-feu et issues de secours<br>☒ Alimentation de secours<br>☒ Installations électriques certifiées et réceptionnées (y compris protection contre les surtensions et distribution d'énergie orientée sur les secteurs)<br>☒Onduleur synchronisé<br>☒ Connexions de télécommunications et de | ☒ Contrôles électriques de tous les appareils électroniques conformément au cycle de contrôle du fabricant<br>☒ Contrôles fonctionnels réguliers<br>☒ Réalisation de la maintenance et de l'entretien par des prestataires de services<br>☒ Rigueur dans le choix des prestataires de services<br>☒ Documentation des Switch-Ports<br>☒ Mises à jour de sécurité<br>☒ Gestion des incidents<br>☒ Gestion du changement |

| | | |
|---|---|---|
| | fournisseurs d'accès via au moins deux connexions en fibre optique et une technique de transfert séparée<br>☒ Connexion redondante de tous les composants importants<br>☒ Révision électrique (VDS)<br>☒ Câblage structuré<br>☒« Armoire réseau » séparée pour la connexion et le réseau<br>☒Système de surveillance informatisé des connexions | ☒ Gestion des urgences informatiques |
| **I.1.2** | **Centre de données interne** | |
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Dispositifs de protection contre l'incendie (notamment par un compartiment séparé de protection contre l'incendie, raccordement à la centrale d'alarme incendie, détecteurs de fumée)<br>☒ Capteurs d'humidité<br>☒ Système d'aspiration des fumées (RAS)<br>☒ Climatisation redondante<br>☒ Installation de remplacement du réseau (NEA, générateur diesel)<br>☒ Alimentation électrique redondante sans coupure<br>☒ Circuits électriques séparés<br>☒ Connexions de télécommunications et de fournisseurs d'accès via au moins deux connexions en fibre optique et une technique de transfert séparée.<br>☒ Connexion redondante de tous les composants importants<br>☒ Révision électrique (VDS)<br>☒ Câblage LAN structuré<br>☒« Armoire réseau » séparée pour la connexion et le réseau<br>☒Système de surveillance informatisé des connexions<br>☒Systèmes de stockage interne redondants<br>☒ Bandes de sauvegarde, conservation des sauvegardes dans un système de stockage redondant dans le centre de données<br>☒Service de sécurité dans un autre lieu | ☒ Concept de sauvegarde et de reprise après sinistre<br>☒Séparation géographique des emplacements de sauvegarde par rapport à l'emplacement du serveur principal<br>☒ Les sauvegardes sont effectuées plusieurs fois par jour (pour les systèmes informatiques internes concernés).<br>☒ Les sauvegardes sont cryptées<br>☒ Tests réguliers de récupération des données et journalisation des résultats<br>☒ Les sauvegardes sont créées via la mise en miroir en temps réel<br>☒ Transport des bandes de sécurité par un service de sécurité<br>☒ Rigueur dans le choix du service de sécurité<br>☒ Mises à jour de sécurité<br>☒ Gestion des incidents<br>☒ Gestion du changement<br>☒ Gestion des urgences informatiques |

## IV. CRYPTAGE ET PSEUDONOMYSATION

☒ Le transfert électronique des échanges par courrier électronique est crypté.
☒ Le transfert électronique de données à caractère personnel ne peut s'effectuer que par des moyens de transfert et de communication cryptés et définis. Le transfert de DONNÉES CLIENTS à caractère personnel non anonymisées (par ex. données de test, de base des collaborateurs, etc.) par des voies de transfert et de communication non définies en commun au préalable n'est pas autorisée.
☒ Le stockage des données à caractère personnel s'effectue sur les systèmes informatiques du client ou dans les services cloud ATOSS.
☒ Le stockage des données à caractère personnel dans les opérations commerciales internes d'ATOSS est crypté.
☒ Toutes les données sur les ordinateurs mobiles et les supports de stockage sont cryptés.
☒ Toutes les technologies de cryptage utilisées en production sont conformes à l'*état de la technique**.
☒ La gestion du matériel clé est définie et documentée pour les systèmes informatiques concernés.
☒ Le cryptage de transport est mis en œuvre exclusivement de bout en bout.
☒ Un ensemble de règles avec des exigences en matière de force et d'algorithme de cryptage et de gestion des clés est mis en œuvre.
☒ Pseudonymisation des données à caractère personnel par des fonctions à sens unique.
☒ Pseudonymisation par des tables de correspondance, celles-ci sont séparées du reste du traitement des données.

**Définition* - L'état de la technique comprend les connaissances techniques acquises jusqu'à la date considérée, qui ont été intégrées dans la pratique de l'entreprise et généralement reconnues.

## V. PROCÉDURES DE CONTROLE, D'EVALUATION ET DE SUIVI REGULIERS

### 1. Gestion de la protection des données

| IV.1 | **Respect et vérification des mesures** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Un contrôle de l'efficacité des mesures de protection techniques et organisationnelles est effectuée au moins une fois par an (audit externe RGPD)<br>☒ Contrôle assisté par outil des formations régulières des collaborateurs et de leur participation | ☒ Délégués internes à la protection des données (les coordonnées sont communiquées sur le **site web ATOSS**)<br>☒ Concept de formation des collaborateurs<br>☒ Sensibilisation régulière des collaborateurs (au moins une fois par an)<br>☒ Respect des obligations d'information conformément aux art. 13 et 14 du RGPD<br>☒ Processus formalisé de traitement des demandes de protection des données et des notifications (également en ce qui concerne l'obligation de notification aux autorités de contrôle)<br>☒ Les analyses d'impact sur la protection des données (AIPD)<br>sont effectuées si nécessaire.<br>☒ Implication des délégués à la protection des données dans les questions de protection des données internes et externes |

**2. Contrôle de la mission**

Mesures garantissant que les données à caractère personnel traitées dans le cadre de cette mission ne peuvent être traitées que conformément aux instructions du CLIENT.

| IV.3 | **Sous-traitants autorisés** | |
|---|---|---|
| | **Mesures techniques** | **Mesures organisationnelles** |
| | ☒ Mesures de sécurité certifiées et documentées des fournisseurs de services (Hosting) | ☒ Rigueur dans le choix des sous-traitants ATOSS<br>☒ Présentation et vérification des preuves des mesures de contrôle et de la conformité au RGPD des fournisseurs de services (Hosting) (p. ex. rapports de contrôle, certificats)<br>☒ Conclusion d'un accord de sous-traitance<br>☒ Documentation des instructions<br>☒ Engagement des sous-traitants ATOSS à la confidentialité et au secret des données<br>☒Conclusion de clauses contractuelles types de l'UE ou d'autres garanties conformément à l'art. 46 du RGPD (si nécessaire)<br>☒ Contrôles continus des sous-traitants en matière de protection des données et de sécurité de l'information<br>☒ Obligation des sous-traitants en cas de transfert vers un pays tiers d'effectuer une évaluation de l'impact du transfert pour les autres sous-traitants et de s'assurer que le résultat de cette évaluation est positif / conforme au RGPD. |

***

**CTD-Annexe III**

- Liste des sous-traitants agréés -

ATOSS dispose de l'autorisation générale du CLIENT pour faire appel à des sous-traitants dont la liste figure dans la présente annexe III du CTD.

ATOSS peut, à tout moment pendant la durée du traitement des données à caractère personnel, choisir et changer de sous-traitant parmi ceux mentionnés dans la présente Annexe III du CTD et donc déjà approuvés par le CLIENT, à sa seule discrétion. ATOSS se réserve le droit de ne pas faire appel à chacun des sous-traitants mentionnés ci-dessous pour le traitement des données à caractère personnel.

| **Entreprise** | **Adresse enregistrée** | **Description de l'activité** | **Remarque** |
|---|---|---|---|
| **Sociétés ATOSS** | | | |
| ATOSS Software SE (Allemagne) | Rosenheimer Str. 141h<br>81671 Munich<br>**Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | ATOSS<br>Filiale<br>(Si non contractant) |
| ATOSS CSD Software GmbH | Rodinger Str. 19<br>93413 Cham<br>**Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | ATOSS<br>Filiale<br>(Si non contractant) |
| ATOSS Software Ges.m.b.H. | Ungargasse 64-66<br>Stiege 3<br>Top 503<br>1030 Vienne<br>**Autriche** | Paramétrage, services de maintenance de logiciels, services de Hotline | ATOSS<br>Filiale<br>(Si non contractant) |
| ATOSS Software AG (Suisse) | Schärenmoosstr. 77<br>8052 Zurich<br>**Suisse** | Paramétrage, services de maintenance de logiciels, services de Hotline | ATOSS<br>Filiale<br>(Si non contractant) |
| SC ATOSS Software SRL | Calea Torontalului 69<br>Timisoara 300668<br>**Roumanie** | Paramétrage, services de maintenance de logiciels, services de Hotline | ATOSS<br>Filiale<br>(Si non contractant) |

| **Les sous-traitants pour les services professionnels** | | | |
|---|---|---|---|
| Accenture N.V/SA | Rue Picard/Picardstraat 11 Boîte/Bus 100 1000 Bruxelles **Pays-Bas** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| AIKAVA GmbH | Amselstr. 15 93413 Cham **Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| b.it³ Business Software+IT GmbH | Birkenstr. 2 5300 Salzbourg / Hallwang **Autriche** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| Bosch Sicherheitssysteme GmbH | Robert-Bosch-Ring 5 85630 Grasbrunn **Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| Capgemini Deutschland GmbH | Potsdamer Platz 5 10785 Berlin **Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| Delaware Consulting CV | Kapel ter Bede 86, 8500 Courtrai **Belgique** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| DELOITTE Consulting GmbH | Dammtorstraße 12 20149 Hambourg **Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| EMPAL GmbH | Bügelestorstr. 7/2 74354 Besigheim **Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |
| Fourtexx GmbH | Grünewalder Str. 28 42657 Solingen **Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants (Si nécessaire pour la fourniture du service) |

| | | | |
|---|---|---|---|
| GZ Gute Zeiten e. K. | Geistenbecker Str. 50<br>41199 Mönchengladbach<br>**Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| Moretime oHG | Sedanstr. 13<br>93055 Regensburg<br>**Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| Ringer Zeiterfassung GmbH & Co. KG | Vollmerstraße 17<br>88400 Biberach a.d. Riss<br>**Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| Robert Schickbauer<br>(On time Consulting) | Schoarerbergstr. 43<br>5302 Henndorf am Wallersee<br>**Autriche** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| SOFT-CONSULT Häge GmbH | Riedheimer Straße 5<br>89129 Langenau<br>**Allemagne** | Paramétrage, services de maintenance de logiciels, services de Hotline | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| **Sous-traitants pour les interfaces** | | | |
| SHAPEiN GmbH | Ruländerweg 10<br>60168 Wiesloch<br>**Allemagne** | Prestataires de services d'interface, y compris les services de maintenance de logiciels | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| Pentos AG | Landsberger Str. 110<br>80339 Munich<br>**Allemagne** | Prestataires de services d'interface, y compris les services de maintenance de logiciels | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| HR Force EDV-Beratung GmbH | Wambachergasse 10<br>1130 Vienne<br>**Autriche** | Prestataires de services d'interface, y compris les services de maintenance de logiciels | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| All for One HR GmbH (Anciennement EMPLEOX GmbH) | Ferdinand-Braun-Str. 24 74074 Heilbronn<br>**Allemagne** | Prestataires de services d'interface, y compris les services de maintenance de logiciels | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |

| | | | |
|---|---|---|---|
| **Sous-traitants pour le matériel informatique** | | | |
| All for One OSC BX GmbH (Anciennement OSC Business Xpert GmbH) | Werftstr. 15<br>30163 Hanovre<br>**Allemagne** | Prestataire de services pour la connexion de composants matériels, y compris les prestations d'assistance/de maintenance et le paramétrage | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| **Sous-traitants pour l'exploitation des SERVICE ATOSS CLOUD** | | | |
| Microsoft Ireland Operations Limited | South County Business Park<br>Leopardstown<br>Dublin 18<br>**Irlande** | Fournisseur d'hébergement incluant des services informatiques gérés (hébergement et exploitation de l'infrastructure cloud) | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| Telekom Deutschland GmbH | Landgrabenweg 151<br>53227 Bonn<br>**Allemagne** | Fournisseur d'hébergement incluant des services informatiques gérés (hébergement et exploitation de l'infrastructure cloud) | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| UMB AG | Müllerenstr. 3<br>8604 Volketswil<br>**Suisse** | Fournisseur d'hébergement incluant des services informatiques gérés (hébergement et exploitation de l'infrastructure cloud) | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |
| Google Ireland Limited | Gordon House<br>Barrow Street<br>Dublin 4<br>**Irlande** | <u>Dans le cas d'ATOSS Mobile Workforce Management (pour fournir un service de messages push :</u><br>Transmission de messages push du module ATOSS Mobile Workforce Management ainsi que de Mobile Employee Self Service User et | Sous-traitants<br>(Si nécessaire pour la fourniture du service) |

| | | | |
|---|---|---|---|
| | | Mobile Manager Self Service User aux utilisateurs de terminaux mobiles | |

***