Accord sur le traitement des données ("DPA") pour les Services Cloud de Unify

En vigueur au janvier 2019

Par et entre le Client ("Client" ou "Responsable du traitement") et Unify Software and Solutions GmbH & Co.KG ("Unify" et " Responsable Conjoint")

Le Client et Unify représentent chacun une "Partie" et, collectivement, les "Parties".

Les Services Cloud de Unify permettent au Client et à ses Utilisateurs de Services Cloud de Unify de saisir des informations pour le traitement par le logiciel fourni en tant que service. Dans la mesure où de telles informations contiennent des Données à caractère personnel, les Parties acceptent expressément que le présent DPA s'applique, selon lequel les deux Parties partagent les rôles et responsabilités en tant que Responsables conjoints du Traitement comme suit :

- Le Client (i) définit seul ou conjointement avec d'autres les fins du Traitement des Données à caractère personnel, (ii) est responsable de l'exactitude des Données à caractère personnel, (iii) est chargé d'informer les personnes concernées du Traitement des Données à caractère personnel et des modalités d'exercice de leurs droits, et (iv) est chargé de notifier les autorités de protection des données (y compris pour les notifications de Violation de la Protection des Données à caractère personnel), le cas échéant.
- Unify (i) définit les moyens du Traitement et (ii) est chargé de la mise en œuvre des mesures de sécurité,

et Unify endosse également le rôle d'Sous-Traitant selon les définitions de la Section 1. Ces rôles et responsabilités sont davantage détaillés dans le Section 4 (Rôles et responsabilités) ci-dessous.

Le présent DPA s'applique à toutes les activités menées par Unify dans le cadre des Services Cloud de Unify et des Conditions de Production du Service (CDPS) publiés par Unify pour ces Services Cloud de Unify , par lesquelles les employés de Unify et les sous-traitants tiers de Unify peuvent être amenés à manipuler des Données à caractère personnel du Client.

Le présent DPA ne s'applique à aucun autre produit, site ou service Unify en ligne ou hors ligne. En ce qui concerne les Services Cloud de Unify, le présent DPA prévaut sur tout autre accord de traitement des données ou arrangement similaire existant entre Unify et le Client qui pourrait déjà être en place pour d'autres produits, sites ou services.

Le Client reconnaît qu'il a reçu toutes les informations qu'il juge nécessaires pour établir le fait que Unify offre des garanties suffisantes en ce qui concerne la protection des Données à caractère personnel.

1. Définitions

En plus des termes définis ailleurs dans les CDPS, les définitions suivantes s'appliquent :

1.1 "Lois applicables à la protection des données personnelles " ou « Loi Applicable »: désigne les lois et réglementations relatives au traitement et à la protection des Données à caractère personnel applicables dans le pays dans lequel Unify est établi. En particulier, la « Loi Applicable » désigne (a) les prescriptions du règlement UE 2016/679 (Règlement général sur la protection des données, RGPD) ; (b) les lois ou réglementations de l'État membre relatives au traitement et à la protection des Données à caractère personnel concernant la mise en œuvre ou en complément du RGPD ; et (c) toute autre loi ou réglementation applicable concernant le traitement et la protection des Données à caractère personnel aux fins de cet Accord.

1.2 "Données à caractère personnel" désigne toute information concernant une personne physique identifiée ou identifiable ("**Personne concernée**") ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs facteurs

propres à l'identité physique, physiologique, psychique, économique, culturelle ou sociale de cette personne.

1.3 "Traitement" ou "Traiter" désigne toute opération ou ensemble d'opérations effectuées sur les Données à caractère personnel, à l'aide ou non de procédés automatisés, telles que la collecte, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la communication par transmission, la diffusion ou tout autre moyen de mettre de telles données à disposition, le rapprochement ou la l'association, la restriction, la suppression ou la destruction.

1.4 "Sous-Traitant" désigne la personne ou l'entité qui Traite les Données à caractère personnel pour le compte du Client comme prévu par l'Accord et le présent DPA.

1.5 "Responsable du traitement" désigne la personne morale ou entité juridique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des Données à caractère personnel. Dans le contexte des Services Cloud de Unify, en vertu du présent DPA, il est convenu, comme indiqué ci-dessus, que les Parties partagent les rôles et responsabilités de Responsables conjoints comme suit :

- Le Client (i) définit seul ou conjointement avec d'autres les fins du Traitement des Données à caractère personnel, (ii) est responsable de l'exactitude des Données à caractère personnel, (iii) est chargé d'informer les personnes concernées du Traitement des Données à caractère personnel et des modalités d'exercice de leurs droits, et (iv) est chargé de notifier les autorités de protection des données (y compris pour les notifications de Violation de la Protection des Données à caractère personnel), le cas échéant.
- Unify (i) définit les moyens du Traitement et (ii) est chargé de la mise en œuvre des mesures de sécurité.

1.6 Violation de la Protection des Données à caractère personnel : désigne la violation d'une mesure de sécurité conduisant de manière accidentelle ou illicite à la destruction, la perte, l'altération, ou la divulgation non autorisée ou l'accès aux Données à caractère personnel du Client qui sont Traitées dans le cadre du présent DPA.

2. Catégories des Données à caractère personnel dans le cadre du présent DPA :

Les catégories suivantes de Données à caractère personnel sont généralement collectées et traitées par Unify pour fournir les Services dans le cadre des CDPS :

- Données de profil : Données à caractère personnel créées par les Utilisateurs de Services Cloud de Unify (Utilisateurs), en particulier leurs noms d'utilisateur, mots de passe, adresses électroniques, droits d'accès.
- Données d'activité : Données à caractère personnel dérivées de l'utilisation de Services Cloud de Unify par l'Utilisateur, en particulier les données du journal d'appels, la suppression de contenu ou les modifications d'enregistrements ou les données liées à l'utilisation du service (par exemple, les paramètres utilisés) par un utilisateur, dans la mesure où de telles données ne sont pas anonymes, afin de générer des Données d'utilisation agrégées.
- Données temporaires ou Données de session : Données à caractère personnel qui ne sont pas stockées dans les Services Cloud de Unify (telles que les informations de présence ou de localisation) ou qui sont liées à une session de connexion aux Services Cloud de Unify (par exemple, les adresses IP).

Sont exclues du présent DPA les Données à caractère personnel que les Utilisateurs de Services Cloud de Unify peuvent saisir dans les Services Cloud de Unify via des publications textuelles, des téléchargements de documents ou des enregistrements vocaux. De telles données ne peuvent pas être reconnues par les Services Cloud de Unify comme Données à caractère personnel. Il est conseillé au Client de gérer l'utilisation desdites Données à caractère personnel de Services Cloud de Unify à l'aide de règles de protection des données appropriées.

3. Catégories de Personnes concernées dans le cadre du présent DPA :

Les catégories suivantes de Personnes concernées sont affectées par le traitement de leurs Données à caractère personnel dans le cadre du présent DPA :

- les Utilisateurs de Location dans la Location des Services Cloud du Client
- les Utilisateurs de Location croisée avec accès à la Location de services Cloud du Client (uniquement les Données d'activité conservées dans la location Services Cloud du Client)

- les utilisateurs de session en tant qu'invité avec accès à la Location de services Cloud du Client

4. Rôles et responsabilités du Client et de Unify

4.1 Rôles et responsabilités du Client :

4.1.1 **Finalités et légalité du Traitement** : le Client est responsable de la définition des finalités du Traitement des Données à caractère personnel, de la légalité du transfert des Données à caractère personnel à Unify et de la légalité du Traitement des données. Le Client doit se conformer, et faire en sorte que ses Filiales et contractants se conforment, à toutes leurs obligations dans le cadre des Lois sur la protection des données lors du traitement des Données à caractère personnel en relation avec les Cloud Services. À cet égard, le Client doit notamment s'assurer d'obtenir et de maintenir toutes les inscriptions et autorisations nécessaires auprès des autorités de protection des données compétentes et de justifier légalement les raisons du traitement des Données à caractère personnel.

4.1.2 **Exercice de leurs droits par les Personnes concernées** : le Client doit être le contact principal des Personnes concernées pour exercer leurs droits conformément aux Lois applicables à la protection des données personnelles. Reportez-vous à l'article 4.2.9 concernantles responsabilités de Unify dans ce contexte.

4.1.3 **Exactitude, qualité, légalité, fiabilité des Données à caractère personnel** : le Client est seul responsable de l'exactitude, de la qualité, de la légalité et de la fiabilité des Données à caractère personnel et des moyens par lesquels il acquiert les Données à caractère personnel pour le traitement par les Services Cloud de Unify.

4.1.4 **Évaluation des risques** : le Client est responsable de l'évaluation des risques résultant du Traitement des Données à caractère personnel.

4.1.5 **Dossiers de traitement :** dans la mesure où cela est requis par la Loi Applicable, le Client est responsable de la conservation et de la tenue des Dossiers de traitement pour les Responsables pour toutes les responsabilités de Responsable du traitement attribuées au Client par le présent DPA. Reportez-vous également aux articles 4.2.1, 4.2.3 et 4.2.14 concernant les responsabilités de Unify dans le présent contexte, ainsi qu'à l'article 4.1.12.

4.1.6 **Informations des Personnes concernées :** le Client est responsable de la fourniture des informations aux Personnes concernées au sujet du Traitement des Données à caractère personnel conformément aux Lois applicables à la protection des données personnelles. Reportez-vous également aux articles 4.2.1 et 4.2.3 concernant les responsabilités de Unify dans le présent contexte, ainsi qu'à l'article 4.1.12.

4.1.7 **Informations concernant la répartition des responsabilités du Responsable du traitement/Responsable conjoint envers les Personnes concernées** : le Client est responsable d'informer les Personnes concernées au sujet de la répartition des responsabilités entre le Responsable du traitement et le Responsable conjoint conformément au présent DPA. Reportez-vous à l'article 4.2.4 concernant les responsabilités de Unify dans le présent contexte.

4.1.8 **Notification de Violation de la Protection des Données à caractère personnel :** le Client doit se conformer à tout devoir de notification de violation de données résultant des exigences applicables en matière de Protection des données personnelles. Lorsque cela est imposé par les Lois applicables à la protection des données personnelles, le Client est responsable de la notification de Violation de la Protection des Données à caractère personnel au Personnes concernées et aux Autorités de protection des données. Reportez-vous également à l'article 4.2.5 concernant les responsabilités de Unify dans ce contexte.

4.1.9 **Modifications de la législation applicable :** le Client doit avertir Unify en temps utile concernant les modifications des réglementations légales susceptibles d'affecter les obligations contractuelles de Unify dans le cadre du présent DPA et qui peuvent nécessiter une modification du présent DPA et de la rémunération convenue. Unify peut également soumettre des propositions au Client si Unify estime qu'une certaine modification est nécessaire pour assurer la

conformité aux Lois Applicables.

4.1.10 **Irrégularités ou erreurs dans le Traitement des Données à caractère personnel :** le Client doit informer Unify de manière immédiate et exhaustive au sujet de toute erreur ou irrégularité liée aux Lois sur la protection des données concernant le Traitement des Données à caractère personnel dont le Client a connaissance.

4.1.11 **Notification des destinataires des Données à caractère personnel concernant la rectification ou la suppression des Données à caractère personnel ou la restriction de Traitement :** Unify ne divulgue pas les Données à caractère personnel à d'autres fins que le Traitement requis pour la fourniture de Services Cloud de Unify (voir section 8). Dans la mesure où le Client divulgue des Données à caractère personnel à un destinataire, par exemple en fédérant les Services Cloud de Unify avec d'autres services cloud de transmission de Données à caractère personnel via des Interfaces de Circuit en dehors du Circuit, le Client est tenu d'informer lesdits destinataires des demandes des Personnes concernées pour la rectification ou la suppression des Données à caractère personnel divulguées ou d'une restriction de Traitement.

4.1.12 **Divulgation des Données à caractère personnel :** Unify divulgue les Données à caractère personnel uniquement aux destinataires auxquels il est nécessaire de divulguer les Données à caractère personnel aux fins de Traitement, selon les modalités précisées dans le document"Informations concernant le Traitement". Certaines fonctionnalités des Services Cloud de Unify permettent aux clients et utilisateurs de divulguer des Données à caractère personnel à des tiers. Dans la mesure où le Client ou les utilisateurs du Client profitent desdites fonctionnalités, le Client est responsable d'informer les Personnes concernées (article 4.1.6) et d'inclure une telle utilisation dans les Dossiers de traitement (article 4.1.5).

4.2 Rôles et responsabilités de Unify

4.2.1 **Moyens de Traitement :** Unify est responsable de définir les moyens de Traitement et, en référence aux articles 4.1.5 et 4.1.6, de fournir les informations concernant ces moyens au Client, en particulier pour permettre au Client de renseigner les Dossiers de traitement et d'informer les Personnes concernées conformément aux Lois applicables à la protection des données personnelles. Se reporter au document "Informations sur le Traitement" pour plus de précisions.

4.2.2 **Champ d'application du Traitement par Unify :** Unify peut collecter et traiter les Données à caractère personnel uniquement dans le cadre du présent DPA et des CDPS applicable aux Services Cloud de Unify fourni au Client et pour améliorer et mettre à niveau de tels services. Les modifications matérielles apportées au champ d'application du Traitement des données doivent être acceptées conjointement et doivent être documentées. Par les présentes, Unify reconnaît expressément qu'elle traitera uniquement les Données à caractère personnel pour la fourniture de Services Cloud de Unify et pour l'amélioration et la mise à niveau de ces Services.

4.2.3 **Mise en œuvre des mesures de sécurité** : Unify est responsable de la mise en œuvre des mesures de sécurité pour le Traitement des Données à caractère personnel dans le cadre des Services Cloud de Unify. Unify prendra les mesures techniques et organisationnelles (MTO) appropriées, telles qu'énoncées dans l'Annexe 1 du présent DPA, conçues pour protéger les Données à caractère personnel du Client contre les abus et les pertes, ou contre toute autre Violation de la Protection des Données à caractère personnel conformément aux Lois applicables à la protection des données personnelles. Le Client comprend que MTO sont soumises aux progrès techniques et développements ultérieurs. À cet égard, Unify est autorisé à utiliser des mesures alternatives appropriées, en informant les Clients en mettant à disposition une description desdites mesures sur demande. En référence aux articles 4.1.5 et 4.1.6, Unify doit fournir les informations concernant les MTO au Client, en particulier pour permettre au Client de renseigner les Dossiers de traitement et d'informer les Personnes concernées conformément aux Lois applicables à la protection des données personnelles.

4.2.4 **Informations sur la répartition aux Parties des responsabilités par rapport aux Personnes concernées :** Unify est responsable de rendre le document DPA standard sans aucune modification accessible à tous les utilisateurs de Services Cloud de Unify. Dans le cas où le présent DPA contient des modifications au document DPA standard demandées par le Client, Unify n'est pas responsable de rendre de telles modifications accessibles aux Personnes concernées.

4.2.5 **Notification de Violation de la Protection des Données à caractère personnel :** dans le contexte de l'article 4.1.8, en cas de Violation de la Protection des Données à caractère personnel , Unify doit aider le Client et fournir toutes les informations nécessaires auxquelles Unify a accès afin de permettre au Client de se conformer à ses obligations. Unify doit informer le Client sans délai de toute Violation de la Protection des Données à caractère personnel du Client découverte par Unify.

4.2.6 **Conservation des Données à caractère personnel/Restriction de suppression :** les Données à caractère personnel traitées par les Services Cloud de Unify sont généralement conservées jusqu'à ce a) qu'elles soient supprimées par le Client ou les utilisateurs de Services Cloud de Unify, ou b) qu'une période de conservation définie par le Client ait expiré, ou c) que l'accord des services cloud du Client sur les Services Cloud de Unify soit résilié (reportez-vous à l'article 4.2.7 sur l'effet de la résiliation). Le Client ne peut pas demander la suppression des Données à caractère personnel dans la mesure où Unify est tenu, en vertu de la loi, de conserver le matériel contenant de telles Données à caractère personnel, par exemple en lien avec toute règle applicable à la conservation des données. Si Unify a besoin de conserver des Données à caractère personnel pour de telles raisons, leur Traitement sera limité par Unify jusqu'à l'expiration de la période de conservation applicable. En outre, le Traitement des Données à caractère personnel doit être restreint plutôt que de supprimer les Données à caractère personnel, dans la mesure légalement permise par les exigences de Protection des données applicables, en particulier si la suppression n'est pas raisonnablement possible ou uniquement possible avec un coût disproportionné en raison du type de stockage particulier. Le Client reconnaît et accepte que certaines demandes puissent entraîner des demandes de rémunération supplémentaires pour Unify. Unify informera le Client en conséquence avant d'exécuter la demande.

4.2.7 **Suppression des Données à caractère personnel et résiliation de l'accord des Services cloud** : Unify est responsable de supprimer toutes les données saisies par le Client et les utilisateurs de Services Cloud de Unify dans les applications logicielles fournies par les Services Cloud de Unify ("Données Location"), notamment les Données à caractère personnel à la fin du mois calendaire suivant l'expiration ou la résiliation de l'utilisation par le Client de Services Cloud de Unify, ou à tout moment à la demande du Client. À la demande du Client, Unify doit fournir un export des Données Location dans un format de données qui peut être traité par le Client pour être transféré vers d'autres services cloud. Pour les exceptions et limitations, consultez l'article 4.2.6.

4.2.8 **Demandes du Client sur les Données à caractère personnel :** Unify est responsable de répondre aux demandes du Client pour la correction, la suppression, la restriction et la mise à disposition des Données à caractère personnel à la fois pendant et à la fin de l'Accord. Pour les exceptions et limitations, consultez l'article 4.2.6.

4.2.9 **Exercice de leurs droits par les Personnes concernées :** en cas de réception par Unify d'une demande d'une Personne concernée à exercer ses droits conformément aux Lois applicables à la protection des données personnelles, Unify doit transmettre ladite demande au Client qui doit en retour donner des instructions à Unify sur la procédure à suivre, sans délai. Le Client reconnaît qu'en cas de conflit entre la Personne concernée et le Client, la législation applicable peut forcer Unify à satisfaire la demande de la Personne concernée contre l'objection du Client. Unify ne prendrait cependant pas une telle mesure sans tenir compte de la situation juridique avec le Client.

4.2.10 **Effets de la suppression des Données à caractère personnel :** par la présente, le Client

confirme et reconnaît que si le Client demande à Unify de supprimer des Données à caractère personnel ou de restreindre leur Traitement, cela pourrait rendre impossible la fourniture des produits ou services fournis ou souscrits. Unify doit avertir le Client de telles conséquences avant l'exécution d'une telle demande.

4.2.11 **Copies de sauvegarde des Données à caractère personnel :** Unify doit effectuer des copies de sauvegarde des Données à caractère personnel dans la mesure où elles sont nécessaires pour assurer le Traitement correct des Données à caractère personnel, et peut copier et conserver les Données à caractère personnel nécessaires à la conformité du Client ou de Unify à ses obligations légales concernant la conservation des documents.

4.2.12 **Manipulation des supports et du matériel d'essai :** Unify doit stocker et manipuler les supports qui lui sont fournis et toutes les copies et reproductions de ceux-ci avec soin afin qu'ils ne soient pas accessibles par des tiers. Unify est tenu d'assurer la destruction du matériel de test et d'autres matériels contenant des Données à caractère personnel qui doivent être jetés d'une manière conforme à la loi seulement sur la base d'une demande individuelle par le Client et à la charge de ce dernier.

4.2.13 **Délégué à la protection des données :** Unify fournira les coordonnées du délégué à la protection des données de Unify (DPO) sur Internet. À compter de la date d'entrée en vigueur du présent DPA, les coordonnées actuelles du DPO sont dp.it-solutions@atos.net.

4.2.14 **Dossiers de traitement :** Unify est responsable de la conservation et de la tenue des Dossiers de traitement pour les obligations du Sous-Traitant et du Responsable conjoint attribuées à Unify par le présent DPA. Reportez-vous également à l'article 4.1.5 concernant les responsabilités du Client dans ce contexte. Les informations sont disponibles dans le document "Information sur le traitement".

5. Accords et responsabilités mutuels

5.1 Les Parties conviennent que toute demande de Données à caractère personnel émise par le Client doit être faite par écrit et de manière explicite. Dans le cas où de telles demandes nécessitent un changement de services, un tel changement doit être renégocié de bonne foi par les deux Parties, ainsi que le prix associé.

5.2 Chacune des Parties doit s'assurer que son personnel respectif est tenu par une obligation légale de respecter les obligations de Protection des données et de préserver la confidentialité des données et qu'il est informé des autres dispositions applicables concernant la protection des Données à caractère personnel, en particulier le secret des télécommunications. L'obligation d'assurer la confidentialité des données se poursuit après la fin de leur travail ou contrat de travail.

5.3 Si Unify estime que la conformité aux demandes du Client pourrait entraîner une violation des Lois applicables à la protection des données personnelles, Unify en informera rapidement le Client. Unify est en droit de suspendre la mise en œuvre de la demande en question jusqu'à ce qu'elle soit confirmée ou modifiée par le Client.

5.4 Les deux Parties reconnaissent par la présente que les mesures de sécurité détaillées à l'Annexe 1 (Mesures techniques et organisationnelles) offrent des garanties suffisantes aux Données à caractère personnel traitées. Le Client comprend que les mesures techniques et organisationnelles sont soumises aux progrès techniques et développements ultérieurs. À cet égard, Unify est autorisé à utiliser des mesures alternatives appropriées.

5.5 Si les Données à caractère personnel du Client font l'objet d'une perquisition et saisie, d'une ordonnance de saisie, d'une confiscation lors d'une procédure de faillite ou d'insolvabilité, ou d'événements ou de mesures similaires de la part d'un tiers, Unify doit informer le Client sans délai, si la loi le permet. Unify doit, sans délai, informer toutes les parties concernées par une telle action que les Données à caractère personnel affectées par leurs mesures sont la seule propriété du Client et à la seule disposition du Client, et que le Client est l'organisme responsable conformément à la Loi Applicable.

6. Demandes des autorités de surveillance

6.1 Lorsque cela est requis par la loi, les deux Parties doivent conserver des enregistrements des Données à caractère personnel traitées aux fins du présent DPA, coopérer et fournir toutes les informations nécessaires pour remplir les obligations et devoirs de notification susmentionnées en vertu des Lois sur la protection des données.

6.2 Si Unify doit aider le Client à respecter les obligations légales du Client telles que stipulées dans cette section 6, le Client doit rembourser à Unify tous les coûts supplémentaires raisonnables associés à la fourniture d'une telle assistance.

7. Droits d'audit

7.1 Au plus une fois par an et sur demande écrite préalable de soixante (60) jours, chaque Partie a le droit de conduire un audit sur la conformité de l'autre Partie au présent DPA, en examinant les mesures techniques et organisationnelles mises en œuvre par la Partie auditée. La preuve de la mise en œuvre de telles mesures qui ne se rapportent pas exclusivement au présent DPA ou à l'Accord peut également être fournie en soumettant un certificat, des rapports ou des extraits de rapports actuels par des tiers indépendants, par exemple des comptables publics certifiés, des auditeurs de compte certifiés, le(s) délégué(s) à la protection des données interne(s) et/ou externe(s) de la Partie auditée, le service de sécurité informatique, les auditeurs internes et externes de protection des données, les auditeurs qualité, ou un certificat approprié émis après que la sécurité informatique ou la protection des données de la Partie auditée a été auditée par un tiers.

7.2 Chaque Partie se réserve le droit de refuser de fournir à l'autre Partie des secrets d'entreprise et de commerce, un savoir-faire opérationnel et toute information dont l'audit présenterait un risque de sécurité pour la Partie auditée ou ses clients ou que la Partie auditée a interdiction de fournir ou divulguer, telle que les données protégées par la loi ou les données d'autres clients.

8. Sous-traitants

8.1 Le Client reconnaît et accepte par la présente que Unify peut engager des sous-traitants pour la fourniture de Services Cloud de Unify. Lesdits sous-traitants peuvent être des entités du groupe Atos ("Sous-traitants internes") ou des sous-traitants tiers ("Sous-traitants externes"). Une liste complète des sous-traitants à la date d'entrée en vigueur du présent DPA est disponible en ligne, y compris les précautions applicables pour la protection adéquate des Données à caractère personnel.

8.2 Les Sous-traitants internes font partie du groupe Atos et sont par conséquent couverts par les Atos Binding Corporate Rules (Règles d'entreprise contraignantes d'Atos) (https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf). En cas d'utilisation de Sous-traitants externes, Unify doit s'assurer que lesdits Sous-traitants externes mettent en œuvre un niveau de protection des Données à caractère personnel similaire aux dispositions énoncées dans le présent DPA.

8.3 Dans le cas où Unify a l'intention d'engager un nouveau Sous-traitant externe qui n'est pas identifié dans la liste des sous-traitants au moment où le présent DPA est accepté par le Client, les articles 9.2 et 9.3 s'appliquent. Afin d'éviter tout doute, il est expressément convenu que les Sous-traitants internes ne seront pas soumis à la présente disposition et que le Client est considéré comme ne s'opposant pas à l'utilisation de Sous-traitants internes.

8.4 Dans le cas où les Données à caractère personnel peuvent être transférées, stockées et traitées dans des pays hors de l'Espace Économique Européen (EEE), par exemple aux États-Unis ou dans tout autre pays où les Filiales ou sous-traitants du Client ou de Unify possèdent des installations, le Client doit s'occuper des accords contractuels nécessaires qui sont requis en vertu des Règlements de l'UE sur la protection des données et de la législation locale applicable pour un transfert ou traitement légalement conforme des Données à caractère personnel. Si, pour se conformer aux Règlements de l'UE sur la protection des données, il est nécessaire d'établir une relation contractuelle directe entre le Client et le sous-traitant, Unify se chargera de la coordination avec le sous-traitant et le Client afin que ce contrat direct soit établi, le présent DPA servant alors de référence.

9. Modifications du présent DPA

9.1 Le Client reconnaît que les conditions du présent DPA et de l'Annexe 1 sont susceptibles d'être modifiées par Unify. Une modification nécessite le consentement du Client si elle a) affecte la répartition des responsabilités entre le Responsable du traitement et le Responsable conjoint conformément à la section 4, ou b) limite les droits du Client, ou c) requiert un consentement conformément à la Loi applicable à la protection des données personnelles. Dans les autres cas, une modification nécessite uniquement d'informer le Client.

9.2 En cas de modification nécessitant le consentement du Client, Unify informera le Client de la modification par courrier électronique à l'administrateur locataire en vertu duquel la location services Cloud du Client est enregistrée auprès de Unify ou via le partenaire commercial accrédité de Unify avec lequel le Client détient l'accord Cloud Services pour un Unify Cloud Service, et mettra les informations pertinentes à la disposition du Client pour examen au moins trente (30) jours calendaires avant l'entrée en vigueur de la modification. Unify donnera au Client la possibilité de donner son consentement ou de s'opposer. Si Unify ne reçoit aucune objection de la part du Client après une période de réponse indiquée sur la notification de modification, qui doit être d'au moins dix (10) jours calendaires suivant la date de notification, le consentement du Client sera considéré comme donné. Dans les situations d'urgence, les périodes de notification et de réponse peuvent être plus courtes.

9.3 Le Client ne doit pas s'opposer à une modification sans fournir à Unify une explication écrite détaillée des motifs d'une telle objection. Unify doit déployer des efforts commercialement raisonnables pour répondre aux préoccupations du Client. Les deux Parties doivent coopérer de bonne foi pour parvenir à un accord. Si aucun accord ne peut être atteint, les Services Cloud de Unify contractés par le Client seront résiliés.

10. Responsabilité

10.1 Unify et le Client doivent s'acquitter de leurs obligations respectives telles qu'énoncées dans le présent DPA et dans la Loi applicable à la protection des données personnelles.

10.2 Le Client est entièrement responsable de tout manquement à ses obligations énoncées à la section 4.1 ci-dessus, ainsi qu'à ses obligations énoncées à la section 5 ci-dessus.

10.3 Unify est entièrement responsable de tout manquement à ses obligations énoncées à la section 4.2 ci-dessus, ainsi qu'à ses obligations énoncées à la section 5 ci-dessus, sous condition de respect par le Client de ses propres obligations.

10.4 En qualité de Sous-Traitant, Unify n'est responsable des dommages causés par le traitement que si Unify n'a pas respecté les obligations de la Loi applicable à la protection des données personnelles pour les Sous-Traitants ou si Unify a agi en dehors ou contrairement aux instructions légales du Client.

10.5 La Partie contrevenante est exonérée de sa responsabilité si elle prouve qu'elle n'est en aucune façon responsable de l'événement à l'origine du dommage.

10.6 Lorsque le Client et Unify sont responsables de tout dommage causé en violation d'une obligation du présent DPA, chaque Partie doit être tenue responsable de l'intégralité du dommage afin d'assurer une compensation efficace de la Personne concernée. La Partie qui a versé la totalité de l'indemnisation pour le dommage subi a le droit de réclamer à l'autre Partie concernée la part de l'indemnisation correspondant à sa part de responsabilité dans le dommage.

11. Divers

11.1 Si une disposition individuelle du DPA est illégale, invalide, nulle, annulable ou inapplicable, le reste du DPA restera pleinement applicable et en vigueur. Les parties conviendront d'une disposition effective qui, dans la mesure légale possible, reflète le plus fidèlement l'intention des Parties.

Annexe 1

Mesures techniques et organisationnelles générales de Unify

Chez Unify, les mesures techniques et organisationnelles requises par la loi sont mises en œuvre sur la base du Cadre de confidentialité des données et de sécurité de l'information de Unify (le " DIS Framework"), qui définit les normes de politique (niveau 2) et les procédures opérationnelles (niveau 3) conformément à la norme internationale ISO27001 sur la base de la politique d'entreprise de Unify "Politique de confidentialité des données et de sécurité de l'information de Unify". Les documents sont accessibles au Client sur demande.

La description suivante du statu quo des mesures élémentaires concernant la protection des données ne peut couvrir toutes les mesures de sécurité en place chez Unify. En particulier dans le contexte de la protection et de la sécurité des données, il est impossible de fournir des descriptions détaillées des mesures confidentielles, car la protection des mesures de sécurité contre la divulgation non autorisée est aussi importante que la mesure de sécurité elle-même.

Le Client est invité à discuter de toute question relative aux mesures techniques et organisationnelles avec le responsable de compte du Client chez Unify, le délégué à la protection des données de Unify et, le cas échéant, le responsable de la sécurité des systèmes d'information (RSSI) de Unify.

1. Contrôle d'entrée

Mesures techniques ou organisationnelles concernant le contrôle d'accès, en particulier concernant la légitimation des personnes autorisées :

Le but du contrôle d'entrée est d'empêcher les personnes non autorisées d'accéder physiquement à un tel équipement de traitement des données qui traite ou utilise des Données à caractère personnel.

En raison de leurs exigences de sécurité respectives, les locaux et installations de l'entreprise sont subdivisés en différentes zones de sécurité avec différentes autorisations d'accès. Elles sont surveillées par le personnel de sécurité. L'accès pour les employés est uniquement possible avec un badge encodé comportant une photo. Toutes les autres personnes ne bénéficient de l'accès qu'après s'être enregistrées (par exemple, à l'entrée principale).

L'accès à des zones de sécurité spéciale telles que le centre de service pour la maintenance à distance est protégé davantage par une zone d'accès séparée. Les normes de sécurité de construction et réelles sont conformes aux exigences de sécurité pour les centres de données.

2. Contrôle d'accès au système

Mesures techniques (protection par mot de passe) et organisationnelles (données principales de utilisateur) concernant l'ID utilisateur et l'authentification :

Le but du contrôle d'accès au système est d'empêcher l'utilisation non autorisée des systèmes de traitement des données qui sont utilisés pour le traitement et l'utilisation des Données à caractère personnel.

Les données principales d'utilisateur et le code d'identification individuel de chaque employé sont enregistrés dans le répertoire de contact global. L'admission aux systèmes de traitement de données n'est possible qu'après identification et authentification à l'aide du code d'identification et du mot de passe pour le système particulier.

Des protections techniques supplémentaires sont en place à l'aide de pare-feu et de serveurs proxy.

Afin de garantir le contrôle d'admission, des technologies de cryptage sont utilisées (par exemple, l'accès distant au réseau de l'entreprise via un tunnel VPN). L'adéquation d'une technologie de cryptage est mesurée par rapport à l'objectif de protection.

3. Contrôle d'accès aux données

Structure à la demande du concept d'autorisation et des droits d'accès aux données ainsi que leur surveillance

et leur enregistrement :

Les mesures concernant le contrôle d'accès aux données doivent être ciblées sur le fait que seules lesdites données pour lesquelles une autorisation d'accès existe sont accessibles et que les Données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées de manière non autorisée pendant le traitement, l'utilisation et après l'enregistrement de telles données.

L'accès aux données nécessaires à l'exécution de la tâche particulière est assuré au sein des systèmes et des applications par un concept de rôle et d'autorisation correspondant. Conformément au principe du "besoin de savoir", chaque rôle ne dispose que des droits nécessaires à l'accomplissement de la tâche par l'individu.

Afin de garantir le contrôle d'accès aux données, une technologie de cryptage est utilisée (par exemple, l'accès distant au réseau de l'entreprise via un tunnel VPN). L'adéquation d'une technologie de cryptage est mesurée par rapport à l'objectif de protection.

4. Contrôle de transmission

Mesures concernant le transport, le transfert, la transmission ou le stockage des Données à caractère personnel sur supports de données (manuellement ou par voie électronique) ainsi que concernant la révision ultérieure :

Le but du contrôle de transmission est de garantir que les Données à caractère personnel ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant leur transfert ou leur stockage sur des supports de données, et qu'elles puissent être surveillées et qu'il puisse être déterminé pour quels destinataires un transfert de Données à caractère personnel est prévu.

Les mesures nécessaires pour assurer la sécurité des données pendant le transport, le transfert et la transmission des Données à caractère personnel ainsi que toutes autres données de l'entreprise ou du client sont détaillées dans la politique sur la protection des informations d'entreprise confidentielles. La présente politique contient une description détaillée de l'ensemble du traitement des données, de la création desdites données à leur suppression, y compris le traitement des données conformément à leur classification.

Afin de garantir le contrôle de transfert, une technologie de cryptage est utilisée (par exemple, l'accès distant au réseau de l'entreprise via un tunnel VPN). L'adéquation d'une technologie de cryptage est mesurée par rapport à l'objectif de protection.

Le transfert des Données à caractère personnel à un tiers (par exemple, des clients, sous-traitants, fournisseurs de services) n'est effectué que si un contrat correspondant existe et uniquement dans un but spécifique. Si les Données à caractère personnel sont transférées à des entreprises dont le siège se trouve en dehors de l'UE/EEE, Unify prévoit qu'un niveau adéquat de protection des données existe sur le site ou l'organisation cible conformément aux exigences de protection des données de l'Union européenne, par exemple en utilisant des contrats basés sur les modèles de clauses contractuelles de l'UE.

5. Contrôle de saisie de données

Mesures concernant l'examen ultérieur, si des données ont été saisies, modifiées ou supprimées, et par qui :

Le but du contrôle de saisie de données est de s'assurer, à l'aide de mesures appropriées, que les circonstances de la saisie des données peuvent être revues et surveillées rétroactivement.

Les entrées du système sont enregistrées sous la forme de fichiers journaux. Ce faisant, il est possible à un stade ultérieur de vérifier si des Données à caractère personnel ont été saisies, modifiées ou supprimées et par qui.

6. Contrôle de traitement des données

Le but du contrôle de traitement des données est de garantir que Unify traite uniquement les Données à caractère personnel conformément aux dispositions des CDPS émises par Unify pour le service cloud sous contrat et aux dispositions stipulées dans l'Accord sur le traitement des données pour les Services Cloud de Unify.

Les Données à caractère personnel traitées dans les Services Cloud de Unify sont uniquement accessibles au support technique et à l'organisation d'exploitation. Unify a mis en place des politiques pour empêcher cette organisation d'utiliser des Données à caractère personnel à d'autres fins ou de divulguer des Informations personnelles à toute autre organisation ou à un tiers, sauf sur instruction du Client.

Un transfert des Données à caractère personnel à un tiers, tel qu'un sous-traitant, est effectué uniquement en tenant compte des dispositions contractuelles et des Lois applicables à la protection des données personnelles.

7. Contrôle de disponibilité

Mesures concernant la sauvegarde des données (physique/logique) :

Le but du contrôle de disponibilité est de garantir que les Données à caractère personnel sont protégées contre la destruction et la perte accidentelles.

Si les Données à caractère personnel ne sont plus nécessaires aux fins pour lesquelles elles ont été traitées, elles sont supprimées rapidement. Il convient de noter qu'à chaque suppression, les Données à caractère personnel sont uniquement verrouillées dans la première instance et sont ensuite définitivement supprimées dans un certain délai. Cela est fait afin d'empêcher des suppressions accidentelles ou des dommages intentionnels possibles.

Pour des raisons techniques, des copies des Données à caractère personnel peuvent être présentes dans les fichiers de sauvegarde et peuvent être réalisées par la mise en miroir des services. Sous réserve de l'obligation statutaire de conservation des données de Unify (voir l'Accord de traitement), de telles copies sont également supprimées (si nécessaire, avec un retard d'origine technique). La disponibilité des systèmes eux-mêmes est assurée conformément au niveau de sécurité requis par des mesures de sécurité correspondantes (par exemple, mise en miroir des disques durs, systèmes RAID, USV).

8. Contrôle de séparation

Mesures concernant le traitement séparé (enregistrement, modification, suppression et transfert) de données à des fins différentes :

Le but du contrôle de séparation est de garantir que les données qui ont été collectées à des fins différentes puissent être traitées séparément.

Les Données à caractère personnel sont utilisées uniquement à des fins internes (par exemple, dans le cadre de la relation client respective). Un transfert à un tiers, tel qu'un sous-traitant, est effectué uniquement en tenant compte des dispositions contractuelles et de la réglementation sur la protection des données.

Les employés sont chargés de collecter, traiter et utiliser les Données à caractère personnel uniquement dans le cadre et aux fins de leurs fonctions (par exemple, la fourniture de services). Sur le plan technique, la capacité multiclient, la séparation des fonctions ainsi que la séparation des systèmes de test et de production sont utilisées à cette fin.