L'ADDITIF DE TRAITEMENT DES DONNÉES MONDIALES

Cet Additif de Traitement des Données Mondiales ((«Annexe» ou «DPA») fait partie du Contrat Cadre, du Bon de Commande ou de tout autre contrat ou document conclu entre le Client et Hyland, qui intègre cette Annexe par référence (le « Document Constitutif »). Tel qu'utilisé dans le présent, le « Contrat » désigne le Document Constitutif, y compris l'Annexe, et tout autre accord dans lequel le Document Constituf est incorporé.

1. DÉFINITIONS.

Tous les termes en majuscules utilisés dans ce DPA auront la signification qui leur est attribuée dans cette Annexe ou, s'ils ne sont pas définis dans ce DPA, l'Annexe des Conditions Générales. Si des termes en majuscules utilisés ici ne sont pas définis dans cette Annexe ou l'Annexe des Conditions Générales, ils auront la signification qui leur est attribuée ailleurs dans ce Contrat. Dans le cas où le même terme défini est défini dans deux (2) Annexes ou plus, le terme sera attribué la signification définie dans chaque Annexe par rapport à ce DPA et, si le terme est également utilisé dans cette Annexe, ce DPA doit être interprétée de manière à inclure toutes les définitions, selon ce que le contexte exige.

«CCT UE» Clauses Contractuelle Types de l'UE désigne la décision d'exécution (UE) 2021/914 de la Commission instaurant des clauses contractuelles types pour les transferts de données à caractère personnel vers des pays tiers.

«Décision d'Adéquation» désigne la décision finale d'un Régulateur, selon laquelle les lois d'un pays tiers offrent un niveau de protection adéquat des Données à Caractère Personnel lorsque celles-ci sont transférées vers ce pays tiers depuis la juridiction de l'autorité gouvernementale concernée.

«Donnée(s) à Caractère Personnel» désigne toute information relative à une Personne Concernée, et protégée en vertu de la Réglementation sur la Protection des Données.

«Donnée(s) à Caractère Personnel du Client» désigne toute Donnée à Caractère Personnel transmise par ou pour le compte du Client dans le cadre de la réalisation des Services.

«Personne Concernée» désigne une personne physique identifiée ou identifiable, telle que définie par la Réglementation sur la Protection des Données applicable.

«Réglementation sur la Protection des Données» désigne toute loi, tout règlement, toute législation ou toute directive applicable au Traitement des Données à Caractère Personnel.

«Régulateur» désigne l'autorité de contrôle ou l'organisme de réglementation compétent en vertu de la Réglementation sur la Protection des Données applicable.

«Traitement» désigne toute opération ou tout ensemble d'opérations effectuées à l'aide de procédés automatisés ou non, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

«Violation de Données à Caractère Personnel» désigne une faille de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés aux Données à Caractère Personnel du Client.

«Services» désigne les services de support technique, les prestations de services, les services relatifs à l'offre hébergée de Hyland, ou de manière générale, tout autre service fourni par Hyland au titre du Contrat-Cadre Hyland.

«Sous-Traitant Ultérieur» désigne une entité qui traite des Données à Caractère Personnel pour le compte de Hyland.

2. TRAITEMENT DE DONNÉES A CARACTÈRE PERSONNEL PAR HYLAND.

2.1 Instructions relatives aux Traitements de Données à Caractère Personnel. Hyland s'engage à Traiter les Données à Caractère Personnel du Client aux seules fins d'exécuter ses obligations au titre du Contrat-Cadre Hyland, et conformément aux termes de l'**Annexe A**, sauf disposition légale contraire. Chaque Partie s'engage à respecter les obligations qui lui incombent au titre de la Réglementation sur la Protection des Données.

2.2 Durée du Traitement. Hyland Traite les Données à Caractère Personnel pour la durée décrite dans l'**Annexe A**.

3. MESURES DE SECURITÉ MISES EN ŒUVRE PAR HYLAND RELATIVES AUX DONNÉES À CARACTÈRE PERSONNEL.

3.1 Mesures Physiques, Techniques et Organisationnelles. Hyland met en œuvre les mesures de sécurité organisationnelles et techniques appropriées afin de protéger les Données à Caractère Personnel du Client contre leur destruction, perte, altération, divulgation ou accès accidentel ou illicite. Ces mesures sont décrites plus en détail dans l'**Annexe B**.

3.2 Traitement par des Sous-Traitants Ultérieurs. Hyland n'a recours qu'aux Sous-Traitants Ultérieurs figurant dans la liste accessible à l'adresse suivante: https://community.hyland.com/en/connect/hyland-sub-processor-list (laquelle peut être mise à jour par Hyland de temps à autre, sans que cette modification ne nécessite un avenant au DPA). Hyland conclut un accord écrit avec chaque Sous-Traitant Ultérieur, comprenant des obligations relatives à la protection des Données à Caractère Personnel du Client au moins aussi protectrices pour les Personnes Concernées que celles prévues dans la Réglementation sur la Protection des Données applicable. Hyland demeure responsable envers le Client des actes ou des

omissions de ses Sous-Traitants Ultérieurs. Hyland informe le Client de tout nouveau Sous-Traitant Ultérieur auquel Hyland entend avoir recours, en mettant à jour la liste susvisée avec les informations relatives à ce dernier; étant précisé que le Client peut s'abonner à la page concernée. Dans la mesure autorisée par la Réglementation sur la Protection des Données, le Client peut s'opposer à ce nouveau Sous-Traitant Ultérieur sous réserve de motifs raisonnables relatifs à des préoccupations de protection des données en notifiant à Hyland (conformément au DPA) cette objection et ses motifs dans un délai de dix (10) jours suivant la réception de la notification de Hyland. En cas d'objection, Hyland peut décider de ne pas avoir recours à ce Sous-Traitant Ultérieur pour traiter les Données à Caractère Personnel du Client. Si Hyland continue à recourir à ce Sous-Traitant Ultérieur à la suite d'une objection raisonnable du Client, ce dernier peut alors choisir de suspendre ou de résilier, sans délai, le Contrat-Cadre Hyland pour ses seules parties affectées par le recours au Sous-Traitant Ultérieur concerné, sur notification adressée à Hyland, et ce sans préjudice des sommes dues à Hyland ou autres droits acquis en vertu du Contrat-Cadre Hyland.

3.3 Confidentialité des Données à Caractère Personnel. Hyland traite les Données à Caractère Personnel du Client comme confidentielles et s'assure que ses personnels (y compris ses prestataires) autorisés à accéder aux Données à Caractère Personnel du Client (i) soient soumis à une obligation de confidentialité contractuelle appropriée, (ii) sont informés de la nature confidentielle des Données à Caractère Personnel du Client, et (iii) ont reçu la formation appropriée concernant les Données à Caractère Personnel du Client.

3.4 Audits Techniques. Hyland autorise le Client à réaliser des audits dans les conditions prévues dans le Contrat-Cadre Hyland. Dans l'hypothèse où le Contrat-Cadre Hyland ne traite pas des audits par le Client, alors, et dans la mesure autorisée par la Réglementation sur la Protection des Données, Hyland autorise le Client, à sa demande raisonnable et dans la limite d'une (1) fois par an, à mener un audit des politiques de sécurité et de confidentialité de Hyland et/ou des registres relatifs au Traitement des Données à Caractère Personnel du Client ou de tout autre élément probant, pouvant être raisonnablement demandé par le Client et permettant de démontrer la conformité de Hyland aux exigences du DPA. Dans la mesure où le Client choisit de mener un audit sur site, celui-ci sera limité aux zones physiques où le Traitement des Données à Caractère Personnel du Client a lieu. Le Client s'engage à ne pas diffuser ou publier à tout tiers (sauf une autorité de contrôle compétente) les produits de travail de l'audit sans l'autorisation écrite et préalable de Hyland. A la discrétion de Hyland et sous réserve d'en notifier préalablement le Client, celui-ci rembourse à Hyland les dépenses et frais raisonnables occasionnés par l'audit, aux tarifs des prestations de services de Hyland en vigueur à cette date (leur liste étant disponible sur demande).Les audits sont soumis aux obligations de confidentialité applicable aux parties. Dans la mesure où le Client fait appel à un tiers indépendant afin de réaliser un audit, les parties conviennent que (i) préalablement à l'audit, ledit auditeur doit conclure avec Hyland, un accord de confidentialité approprié, et que (ii) tous rapports ou informations de Hyland collectés au cours de l'audit ne peuvent être utilisés que pour les besoins internes du Client.

3.5 Restitution ou Destruction des Données à Caractère Personnel. Hyland s'engage à supprimer ou restituer les Données à Caractère Personnel du Client dans les conditions prévues par le Contrat-Cadre Hyland. Dans l'hypothèse où le Contrat-Cadre Hyland ne traite pas de la suppression ou la restitution des Données à Caractère Personnel du Client, et sur demande écrite du Client, Hyland prend les dispositions nécessaires pour assurer la restitution prompte et sécurisée et/ou à la suppression définitive de toutes les Données à Caractère Personnel du Client en sa possession et sous son contrôle, en ce compris –le cas échéant– toutes copies, dans un délai de vingt-huit (28) jours à compter de la demande du Client et, sur demande du Client, certifie la réalisation de cette suppression. Les engagements de Hyland en termes de protection des Données à Caractère Personnel au titre du DPA continuent à s'appliquer jusqu'à la restitution et/ou la suppression des Données à Caractère Personnel du Client.

3.6 Demandes Adressées à Hyland. Dans la mesure autorisée par la loi, Hyland notifie au Client dans les meilleurs délais (et en tout état de cause dans les quarante-huit (48) heures) suivant sa réception: (a) toute demande réelle ou présumée, d'une Personne Concernée exerçant ses droits en vertu de la Réglementation sur la Protection des Données applicable, ou formulée pour son compte (la «Demande de la Personne

Concernée»); ou (b) toute correspondance ou communication d'un Régulateur (la «Correspondance du Régulateur»). A moins que la loi applicable n'en dispose autrement, Hyland ne transmet aucune Donnée à Caractère Personnel du Client en réponse à une telle demande sans l'instruction écrite et préalable du Client.

3.7 Demandes d'Informations en Vue d'une Analyse d'Impact. A la demande raisonnable du Client, et dans la mesure où il ne peut accéder à l'information concernée par d'autres moyens pour remplir ses obligations au titre de la Réglementation sur la Protection des Données, Hyland s'engage à coopérer raisonnablement et à apporter son assistance au Client, dans la mesure nécessaire, pour la réalisation de toute analyse d'impact sur la vie privée ou sur la protection des Données à Caractère Personnel, imposée par la Réglementation sur la Protection des Données et relative à l'utilisation des Services par le Client. A la discrétion de Hyland et sous réserve d'en notifier préalablement le Client, celui-ci rembourse à Hyland les frais raisonnables liés à sa demande et supportés par Hyland, selon les tarifs des prestations de services de Hyland en vigueur à cette date (leur liste étant disponible sur demande).

3.8 Notification des Violation de Données à Caractère Personnel. Hyland notifie au Client toute Violation de Données à Caractère Personnel dans les meilleurs délais après en avoir pris connaissance. Hyland fait ses meilleurs efforts pour identifier la cause de la Violation de Données à Caractère Personnel et prend les mesures qu'elle estime nécessaires et raisonnables pour y remédier. En outre, et compte-tenu de la nature du Traitement et des informations à sa disposition, Hyland assiste le Client dans le cadre de ses obligations de notification, conformément à la Réglementation sur la Protection des Données. Toute notification effectuée par Hyland en vertu du présent article ne saurait être interprétée comme la reconnaissance, par Hyland, d'une faute de sa part.

4. OBLIGATIONS DU CLIENT RELATIVES AUX DONNÉES À CARACTÈRE PERSONNEL.

4.1 Le Client s'engage à respecter ses obligations relatives aux notifications à des tiers, en les réalisant, conformément à la Réglementation sur la Protection des Données, de manière objective et sans intentionnellement ou déraisonnablement porter préjudice à Hyland ou à sa réputation.

4.2 Le Client garantit qu'il n'est pas soumis à une quelconque interdiction ou restriction qui: (i) l'empêcherait ou limiterait son droit de divulguer ou de transférer les Données à Caractère Personnel du Client à Hyland; (ii) l'empêcherait ou limiterait son droit d'accorder à Hyland l'accès aux Données à Caractère Personnel du Client; et/ou (iii) empêcherait ou restreindrait le droit de Hyland de Traiter les Données à Caractère Personnel du Client, dans la mesure nécessaire pour réaliser les Services.

4.3 Le Client garantit avoir diffusé les mentions d'information requises (et avoir obtenu, si nécessaire, le consentement des Personnes Concernées) et suffisantes pour permettre à Hyland de Traiter les Données à Caractère Personnel du Client en conformité avec la Réglementation sur la Protection des Données.

4.4 Le Client garantit que toutes les Données à Caractère Personnel divulguées ou transmises à Hyland sont strictement nécessaires à la réalisation des Services.

4.5 Le Client s'engage à mettre en œuvre et maintenir les mesures de sécurité techniques et organisationnelles raisonnables et appropriées afin d'empêcher tout accès non autorisé aux Services par le biais des systèmes d'information du Client.

4.6 Le Client est seul responsable de l'exactitude, de la qualité et de la légalité des Données à Caractère Personnel du Client transmises à Hyland et des moyens par lesquels le Client a acquis ces Données à Caractère Personnel.

5. CONDITIONS SPÉCIFIQUES À LA JURISDICTION.

5.1 L'Addendum I, incorporé aux présentes, s'applique lorsque (a) le Client est (i) situé dans l'Espace Économique Européen (l'«EEE»), ou (ii) contracte au nom de tout membre de son propre groupe situé dans l'EEE; et (b) Hyland Traite des Données à Caractère Personnel à partir d'un pays ne faisant pas l'objet d'une Décision d'Adéquation.

5.2 Le Client reconnait et accepte que les Sous-Traitants Ultérieurs de Hyland peuvent être situés en dehors de l'EEE, y compris aux Etats-Unis. Le cas échéant, Hyland met en œuvre et se conforme aux CCT UE pour l'ensemble des transferts qu'elle effectue (en tant qu'exportateur de données) vers un Sous-Traitant Ultérieur (en tant qu'importateur de données) situé dans une juridiction hors de l'EEE et ne faisant pas l'objet d'une Décision d'Adéquation.

6. DURÉE ET RÉSILIATION.

6.1 Durée. Le DPA prend effet à compter de la Date d'Entrée en Vigueur et prend fin automatiquement à la résiliation ou à l'expiration du Contrat Cadre Hyland.

6.2 Effets. A la fin du DPA, Hyland restitue ou détruit les Données à Caractère Personnel du Client, tel que prévu ci-avant.

7. STIPULATIONS GÉNÉRALES.

7.1 Modifications. Les parties conviennent que le DPA peut être occasionnellement modifié afin de permettre aux parties de rester en conformité avec la Réglementation sur la Protection des Données applicable.

7.2 Conflit. Le présent DPA remplace toute disposition incompatible dans le Contrat Cadre Hyland et/ou d'autres contrats existants entre Hyland et le Client en ce qui concerne les obligations des parties de se conformer avec la Réglementation sur la Protection des Données en ce qui concerne les Donnée(s) à Caractère Personnel du Client. En cas de conflit entre le présent Contrat, le(s) Contrat(s) Cadre(s) Hyland et les conditions d'un Addendum applicable, les conditions de l'Addendum applicable prévaudront en ce qui concerne les Donnée(s) à Caractère Personnel soumises à cet Addendum.

8. LANGUE DE CONTRÔLE. Hyland peut mettre à disposition d'autres versions de cette Annexe dans d'autres langues sur cette adresse en ligne. Cette version en anglais de cette Annexe prévaut sur toute version de cette Annexe mise à la disposition sur cette adresse en ligne dans une autre langue si le Document Constitutif est en anglais. Si le Document Constitutif est rédigé dans une langue autre que l'anglais (cette langue, l' « Autre Langue »), cependant cette Annexe n'est pas mise à disposition sur cette adresse en ligne dans l'Autre Langue ; la version de langue anglaise prévaut sur toute autre version de cette Annexe qui peut être mise à disposition sur cette adresse en ligne dans une autre langue.

ADDENDUM 1

EEE

Les parties accordent que les transferts de Données à Caractère Personnel du Client depuis l'EEE seront régis par les CCT UE applicables (telles que complétées par les présentes), lesquelles sont intégrées au DPA par référence.

Les parties conviennent en outre que les CCT UE seront complétées comme suit:

- Le Module 2 s'applique, sauf dans le cas où le Client est un Sous-Traitant, auquel cas le Module 3 s'applique.
- La clause d'adhésion facultative prévue par l'article 7 ne s'applique pas.
- Dans le cadre de l'article 9(a), l'option 2 s'applique. Le Client autorise Hyland à engager des Sous-Traitants Ultérieurs dans les conditions décrites par le DPA.
- Les voies de recours optionnelles prévues par l'article 11 ne s'appliquent pas.
- Dans le cadre de l'article 17, l'option 1 s'applique. Les CCT UE sont régies par le droit applicable au Contrat Cadre Hyland, tel qu'il y est stipulé, sous réserve que ce droit soit celui d'un État Membre de l'UE reconnaissant les tiers bénéficiaires; à défaut, le droit des Pays-Bas s'applique.
- Dans le cadre de l'article 18(b), les litiges sont résolus devant la juridiction compétente au titre du Contrat Cadre Hyland sous réserve que cette juridiction soit située dans un État Membre de l'UE reconnaissant les tiers bénéficiaires; à défaut, les tribunaux des Pays-Bas sont compétents.
- L'annexe I des CCT UE est réputée complétée par les informations figurant à l'Annexe A.
- L'annexe II des CCT UE est réputée complétée par les informations figurant à l'Annexe B.
- L'annexe III des CCT UE est réputée complétée par les informations applicables figurant à l'Annexe A.
- La signature du Contrat emporte toute signature nécessaire des CCT EU, en ce compris les Annexes ci-après.

Annexe A

Objet et Durée du Traitement	L'objet du Traitement est l'exécution, par Hyland, de ses obligations au titre du Contrat Cadre Hyland. La durée du Traitement est la durée du Contrat Cadre Hyland augmentée de toute période de sortie, le cas échéant.
Catégories de Personnes Concernées	Toute Personne Concernée dont les Données à Caractère Personnel sont transmises à Hyland au titre du Contrat Cadre Hyland, et qui peut relever des catégories suivantes:

	• Salariés du Client (personnels passés, potentiels, présents et futurs du Client) • Partenaires du Client (conseillers, consultants, vendeurs, entrepreneurs, sous-traitants et autres professionnels engagés par le Clients par le passé, présents et potentiels, ainsi que leurs personnels) • Utilisateurs Finaux du Client (utilisateurs passés, présents et potentiels, des services et produits du Client)
Nature et Finalité du Traitement	La finalité du Traitement est de fournir les Services et de permettre à Hyland d'exécuter ses obligations en vertu du Contrat Cadre Hyland. La nature du Traitement peut inclure, sans que cette liste ne soit exhaustive, la collecte, l'enregistrement, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
Catégories de Données à Caractère Personnel Traitées	Toute Donnée à Caractère Personnel transmise par le client à Hyland en vertu du Contrat Cadre Hyland.
Catégories de Données à Caractère Personnel sensibles Traitées	☐ Aucun traitement de Données à Caractère Personnel sensibles par Hyland n'est prévu. ☐ Le Client fournit des Données à Caractère Personnel sensibles appartenant aux catégories suivantes à Hyland dans le cadre du Contrat Cadre Hyland.
POUR LES CCT UE UNIQUEMENT	
Exportateur de Données (et pays dans lequel celui-ci est établi)	Le Client, tel que défini dans le DPA.
Importateur de Données (et pays dans lequel celui-ci est établi)	Hyland, tel que défini dans le DPA.
Fréquence du/des	De manière continue (services liés aux offres hébergées ou aux services cloud Hyland);

Transfert(s)	De manière ponctuelle (support technique, prestations de services ou autres services applicables).
Durée de Conservation	Pour les clients des services d'hébergement ou cloud, les données sont conservées pendant la durée du Contrat-Cadre Hyland, en ce compris toute période de transition applicable, sous réserve de toute période plus courte que le Client peut choisir en supprimant définitivement les Données à Caractère Personnel des Services. Les Données à Caractère Personnel transmises à Hyland pour les besoins du support technique ou des prestations de services sont conservées pendant une durée n'excédant pas celle nécessaire aux fins pour lesquelles les Données à Caractère Personnel ont été transmises et, en aucun cas, plus longtemps que ce qui est autorisé par les lois du pays où est établi l'exportateur de données.
Sous-Traitants Ultérieurs	L'importateur de données peut avoir recours aux Sous-Traitants Ultérieurs énumérés à l'adresse suivante: https://community.hyland.com/en/connect/hyland-sub-processor-list.
Autorité de contrôle compétente	L'autorité de contrôle compétente est l'autorité de contrôle compétente de l'État Membre de l'UE/EEE où l'Exportateur de Données est établi.

Annexe B

Mesures Techniques et Organisationnelles

En tenant compte:

- de l'état de l'art,
- des coûts de mise en œuvre et
- de la nature, de la portée, du contexte et
- des finalités du traitement ainsi que
- des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité sont variables,

Hyland met en œuvre les mesures techniques et organisationnelles énoncées dans le Contrat Cadre Hyland. Dans la mesure où le Contrat Cadre Hyland ne spécifie pas les mesures de sécurité techniques et organisationnelles applicables, Hyland met en œuvre les mesures de sécurité techniques et organisationnelles énoncées dans la présente Annexe B comme suit:

1. Mesures relatives au chiffrement.

- chiffrement des appareils mobiles tels que les ordinateurs portables, les tablettes et les smartphones
- chiffrement des supports de stockage mobiles (CD/DVD- ROM, clés USB, disques durs externes)

- stockage crypté des mots de passe
- option de chiffrement des e-mails et pièces jointes sensibles
- partage sécurisé des données (par ex. SSL, FTPS, TLS)
- WLAN sécurisé

2. Mesures visant à garantir la confidentialité.

a. Les mesures garantissant qu'une personne non autorisée ne peut avoir accès aux Données à Caractère Personnel du Client:

- système de contrôle d'accès, lecteur de documents (carte magnétique / à puce)
- protection des portes (ouvre-porte électrique, serrure à chiffres, etc.)
- protection des installations, y compris les gardes de sécurité au siège social de Hyland
- système d'alarme
- surveillance vidéo
- mesures de protection spéciales pour la salle des serveurs
- zones dont l'accès est restreint à certaines catégories de salariés ou consultants
- règles relatives aux visiteurs (par exemple, prise en charge à la réception, documentation des heures de visite, carte de visiteur, accompagnement des visiteurs à la sortie après la visite).

b. Les mesures visant à empêcher une personne non autorisée à utiliser les systèmes traitant les Données à Caractère Personnel du Client:

- connexion personnelle et individuelle des utilisateurs pour l'enregistrement dans les systèmes ou le réseau de l'entreprise
- processus d'autorisation d'accès
- limitation des utilisateurs autorisés
- authentification unique
- authentification à deux facteurs
- mots de passe BIOS pour les ordinateurs portables d'entreprise
- procédures relatives aux mots de passe (indication des paramètres des mots de passe en ce qui concerne leur complexité et l'intervalle de leur mise à jour)
- journalisation des accès
- système de connexion supplémentaire pour certaines applications
- verrouillage automatique des appareils après l'expiration d'une certaine période sans activité de l'utilisateur (également économiseur d'écran protégé par mot de passe ou mise en veille automatique)
- pare-feu

c. Mesures assurant que seules les personnes autorisées ont accès aux systèmes traitant les Données à Caractère Personnel du Client et que celles-ci ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation:

- évaluations/journalisation du traitement des données
- processus d'autorisation pour les autorisations
- routines d'approbation

- profils / rôles
- chiffrement au repos et en transit des Données à Caractère Personnel du Client transférées à Hyland via son outil de transfert de fichiers sécurisé.
- système de gestion des appareils mobiles pour les appareils mobiles appartenant à l'entreprise et les appareils mobiles personnels approuvés (les appareils mobiles ne font pas partie de la solution hébergée)
- séparation des fonctions "segregation of duties" (séparation des tâches)
- destruction des dossiers et des dispositifs de stockage conformément à la norme NIST 800-88, le cas échéant
- journalisations liées à la cybersécurité conservées pendant au moins six mois

3. Mesures visant à assurer l'intégrité.

- droits d'accès
- journalisation côté système
- système de gestion des documents (SGD) avec historique des modifications
- logiciel de sécurité / journalisation
- responsabilités fonctionnelles, responsabilités organisationnelles spécifiques
- connexions de données à distance par tunnel (VPN = réseau privé virtuel)
- signature électronique
- journalisation du transfert ou du transport des données
- journalisation des accès en lecture

4. Mesures visant à assurer et restaurer la disponibilité.

- concept de sécurité pour les logiciels et les applications informatiques
- procédures de sauvegarde, le cas échéant
- stockage des données dans un réseau sécurisé
- installation des mises à jour de sécurité en fonction des besoins
- mise en place d'une alimentation électrique ininterrompue
- installations d'archivage appropriées pour les documents papier
- protection contre le feu et/ou l'eau d'extinction pour la salle des serveurs
- salle des serveurs climatisée
- protection contre les virus
- pare-feu
- plan de continuité des activités
- exercices de reprise après sinistre réussis
- stockage des données redondant et séparé localement (stockage hors site), le cas échéant

5. Mesures pour assurer la résilience.

- plan d'urgence en cas de panne de machine / plan de reprise d'activité

- alimentation électrique redondante
- capacité suffisante des systèmes informatiques et des installations
- processus logistiquement contrôlé pour éviter les pics de puissance
- systèmes / installations redondants
- gestion de la résilience et des erreurs

6. Procédure d'examen, d'évaluation et de contrôle réguliers de l'efficacité des mesures techniques et organisationnelles.

- procédures de contrôles/audits réguliers
- concept d'examen, d'appréciation et d'évaluation réguliers
- système de rapports
- tests de pénétration
- tests d'urgence
- certifications applicables

7. "Contrôle des instructions / contrôle des missions".

- processus d'émission et/ou de suivi des instructions
- spécification des personnes de contact et/ou des employés responsables
- contrôle / examen que l'affectation est exécutée conformément aux instructions
- formation / instruction de tous les employés autorisés à accéder au site
- audit indépendant du respect des instructions
- engagement de confidentialité des salariés
- accord sur les sanctions en cas de violation des instructions
- responsable / coordinateur de la protection des données
- tenir des registres des activités de traitement conformément à l'art. 30, paragraphe 2 du RGPD, le cas échéant
- Politique de Réponse aux Incidents de Sécurité documentée, qui comprend des processus d'escalade pour les Violations de Données à Caractère Personnel
- lignes directrices / instructions visant à garantir des mesures technico-organisationnelles pour la sécurité du traitement
- processus de transmission des demandes des personnes concernées

La version la plus récente de ce document sera en vigueur à 12h00 HNE (Heure Normale de l'Est) de la date apposée sur cette version en ligne.