

ANNEXE

Clauses contractuelles types Responsable du traitement / Sous-traitant

Modèle de la Commission européenne issu de la DÉCISION D'EXÉCUTION (UE) 2021/915

Les présentes clauses contractuelles types peuvent, le cas échéant, être complétées par des clauses ou des garanties supplémentaires à conditions que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses contractuelles types et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées comme précisé dans la décision d'exécution (UE) 2021/915 de la Commission européenne.

SECTION I : DISPOSITIONS GENERALES

Clause 1 : Objet et champ d'application

- a) Les présentes clauses contractuelles types (ci-après les « clauses ») ont pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.
- c) Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II.
- d) Les annexes I à IV font partie intégrante des clauses.
- e) Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
- f) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

Clause 2 : Invariabilité des clauses

- a) Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.
- b) Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Clause 3 : Interprétation

- a) Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 ou dans le règlement (UE) 2018/1725 figurent dans les clauses, ils s'entendent comme dans le règlement en question.
- b) Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 respectivement.
- c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 / le règlement (UE) 2018/1725 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Clause 4 : Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

Clause 5 : Clause d'amarrage

- a) Toute entité qui n'est pas partie aux présentes clauses peut, avec l'accord de toutes les parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l'annexe I.
- b) Une fois que les annexes mentionnées au point a) sont complétées et signées, l'entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d'un responsable du traitement ou d'un sous-traitant, conformément à sa désignation à l'annexe I.
- c) Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l'adhésion.

SECTION II : OBLIGATIONS DES PARTIES

Clause 6 : Description du ou des traitements

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 pour le compte du responsable du traitement, sont précisés à l'annexe II.

Clause 7 : Obligations des parties

7.1. Instructions

- a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.
- b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II.

7.4. Sécurité du traitement

- a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, 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 personnes concernées.
- b) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

7.6. Documentation et conformité

- a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.
- b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.

- c) Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.
- d) Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.
- e) Les parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

7.7. Recours à des sous-traitants ultérieurs

- a) **AUTORISATION ÉCRITE GÉNÉRALE** : le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins quinze (15) jours ouvrés à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.
- b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
- c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.
- d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
- e) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

7.8. Transferts internationaux

- a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de

satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.

- b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

Clause 8 : Assistance au responsable du traitement

- a) Le sous-traitant informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.
- b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.
- c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :
 - 1) L'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d'impact relative à la protection des données ») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;
 - 2) L'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
 - 3) L'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;
 - 4) Les obligations prévues à l'article 32 du règlement (UE) 2016/679.
- d) Les parties définissent à l'annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

Clause 9 : Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles 34 et 35 du règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

9.1. Violation de données en rapport avec des données traitées par le responsable du traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement :

- a) Aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques) ;
- b) Aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679 doivent figurer dans la notification du responsable du traitement, et inclure, au moins :
 - 1) La nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
 - 2) Les conséquences probables de la violation de données à caractère personnel ;
 - 3) Les mesures prises ou les mesures que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;

- c) Aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

9.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

- a) Une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;
- b) Les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
- c) Ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent à l'annexe III tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679

SECTION III : DISPOSITIONS FINALES

Clause 10 : Non-respect des clauses et résiliation

- a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
- b) Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :
 - 1) Le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
 - 2) Le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725 ;
 - 3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
- c) Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.
- d) À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

ANNEXE I : LISTE DES PARTIES

Responsable(s) du traitement :

Nom :

Adresse :

Information relative au Nom, fonction et coordonnées de la personne de contact :

Signature et date d'adhésion :

Sous-traitant(s) :

Nom : KYDOC

Adresse : 60 quai Perrache, 69002 Lyon (siège social 40, rue des Geltines 69390 Millery)

Nom, fonction et coordonnées de la personne de contact : contact@kydoc.fr

Signature et date d'adhésion :

ANNEXE II : DESCRIPTION DU TRAITEMENT

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

- Utilisateurs de la plateforme KYDOC :
 - o Salariés du client responsable de traitement (signataire des documents hébergés sur la Plateforme ;
 - o Titulaire d'un compte sur la plateforme.

Catégories de données à caractère personnel traitées :

- Données d'identification (nom, prénom, genre) ;
- Données de contact (adresse postale, adresse e-mail, numéro de téléphone) ;
- Données professionnelles (titre, employeur, classification, matricule, périmètre de la délégation, rattachement hiérarchique).

Les données sensibles traitées (le cas échéant) et les limitations ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, tels que, par exemple, la limitation stricte de la finalité, les restrictions des accès (y compris l'accès réservé uniquement au personnel ayant suivi une formation spécialisée), la tenue d'un registre de l'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

- Non applicable

Nature du traitement :

- Accès ;
- Enregistrement ;
- Hébergement ;
- Consultation ;
- Utilisation ;
- Collecte ;
- Communication ;
- Destruction / effacement.

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

- Fourniture de la prestation décrite dans les conditions générales de vente de services et d'utilisation de la plateforme KYDOC notamment à l'article 5.1 – fonctionnalité de la plateforme.

Durée du traitement :

- Durée de la réalisation de la prestation telle que décrite dans les conditions générales de vente de services et d'utilisation de la plateforme KYDOC.

Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement :

- Objet : centre d'hébergement du sous-traitant ;
- Nature : hébergement des données ;
- Durée : durée de réalisation de la prestation.

ANNEXE III : MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT A GARANTIR LA SECURITE DES DONNEES

I - Description des mesures techniques et organisationnelles mises en place par KYDOC :

- Information et sensibilisation des personnes manipulant les données ;
- Définition d'un identifiant (login) unique à chaque utilisateur ;
- Utilisation de mot de passe conforme aux recommandations de la CNIL (<https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>) ;
- Verrouillage automatique de session ;
- Utilisation d'un antivirus régulièrement mis à jour et d'un firewall ;
- Sauvegardes ou des synchronisations régulières des données (via Microsoft) ;
- Mise en place d'un secret pour le déverrouillage des smartphones ;
- Mise en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi ;
- Effacement des données de tout matériel avant sa mise au rebut ;
- Mise en place d'une clause de sous-traitance ou d'un accord relatif aux traitements des données avec les sous-traitants ayant accès aux données à caractère personnel ;
- Chiffrement des données avant leur envoi ;
- Accès sécurisé aux bâtiments (via badge d'accès individuel).

II - Descriptions des mesures techniques et organisationnelles mises en place par le sous-traitant ultérieur MICROSOFT (utilisation de la suite Windows 365, rétention du code source, gestion de projets et hébergement sur cloud Azure) :

Le Services Data Protection Addendum (DPA) de Microsoft est accessible via ce lien :

<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=13>

Extrait des mesures de sécurité mises en œuvre par Microsoft (version à jour au 2 Janvier 2024) :

Domaine	Pratiques
Organisation de la sécurité des informations	Responsabilité de la Sécurité. Microsoft charge au moins un agent de coordonner et contrôler les règles et procédures de sécurité. Rôles et Responsabilités en Matière de Sécurité. Le personnel de Microsoft accédant aux Données Client ou aux Données des Services Professionnels est soumis à une obligation de confidentialité. Programme de Gestion des Risques. Microsoft a procédé à une évaluation des risques avant de traiter les Données Client ou de lancer les Services en Ligne et avant de traiter les Données des Services Professionnel ou de lancer les Services Professionnels. Microsoft conserve ses documents de sécurité au-delà de la durée fixée par les exigences de rétention applicables.

Domaine	Pratiques
Asset Management (gestion des ressources)	Inventaire des Ressources. Microsoft conserve un inventaire de tous les supports sur lesquels les Données Client ou les Données des Services Professionnels sont stockées. L'accès à ces inventaires est restreint au personnel de Microsoft autorisé par écrit. Gestion des Ressources - Microsoft classe les Données Client et les Données des Services Professionnels pour faciliter leur identification et la restriction de l'accès à ces données. - Microsoft impose des restrictions au regard de l'impression des Données Client et des Données des Services Professionnels et des procédures de mise au rebut de ces imprimés contenant ce type de données. - Le personnel de Microsoft doit obtenir l'autorisation de Microsoft avant de stocker des Données Client et les Données des Services Professionnels sur des dispositifs portables, d'accéder à distance à ces données ou de traiter ces données en dehors des locaux de Microsoft.
Sécurité des ressources humaines	Formation à la Sécurité. Microsoft informe son personnel des procédures de sécurité applicables et du rôle connexe de chaque employé. Microsoft informe également son personnel des conséquences possibles d'un manquement aux règles et procédures. Microsoft n'utilise que des données anonymes dans le cadre de la formation de son personnel.
Sécurité physique et environnementale	Accès Physique aux Locaux. Microsoft limite l'accès aux locaux qui contiennent des systèmes informatiques traitant des Données Client ou des Données des Services Professionnels aux seuls membres autorisés de son personnel. Accès Physique aux Supports. Microsoft conserve des registres des entrées et sorties des supports qui renferment des Données Client ou des Données des Services Professionnels, où sont décrits le type de support, l'identité des expéditeurs/destinataires autorisés, la date et l'heure, le nombre de supports et les types de données qu'ils contiennent. Protection Contre les Interruptions de Service. Microsoft utilise plusieurs systèmes de protection contre la perte de données après panne de courant ou interférences électriques, conformes aux normes de l'industrie. Mise au Rebut des Supports. Microsoft supprime les Données Client et les Données des Services Professionnels obsolètes au moyen de procédures conformes aux normes de l'industrie.
Gestion des communications et des opérations	Politique Opérationnelle. Microsoft conserve les documents de sécurité décrivant les mesures de sécurité et procédures applicables, ainsi que les responsabilités des membres de son personnel ayant accès aux Données Client ou aux Données des Services Professionnels. Procédures de récupération de données - De manière régulière, mais en aucun cas moins d'une fois par semaine (à moins qu'aucune mise à jour n'ait eu lieu pendant cette période), Microsoft conserve plusieurs copies des Données Client et des Données des Services Professionnels à partir desquelles ces données peuvent être récupérées. - Microsoft stocke les copies des Données Client et des Données des Services Professionnels et les procédures de récupération de données dans un lieu distinct de celui renfermant les équipements informatiques principaux qui traitent les Données Client et les Données des Services Professionnels. - Microsoft applique des procédures spécifiques régissant l'accès aux copies des Données Client et des Données des Services Professionnels. - Microsoft examine ses procédures de récupération de données chaque semestre au minimum, excepté pour les procédures de récupération de données pour les Services Professionnels et pour le Secteur Public Azure, qui sont réévaluées tous les douze (12) mois.

Domaine	Pratiques
	- Microsoft consigne ses tâches de restauration de données dans des journaux, en indiquant le nom de la personne responsable, les données restaurées et, le cas échéant, le nom de la personne responsable et les données (le cas échéant) ayant dû être saisies manuellement au cours de la procédure de récupération. Logiciels Malveillants. Microsoft a mis en place des mesures de lutte contre les logiciels malveillants afin de protéger les Données Client et les Données des Services Professionnels contre les tentatives d'accès non autorisées, y compris des logiciels malveillants issus des réseaux publics. Données transitant Hors du Réseau de Microsoft - Microsoft chiffre ou permet au Client de chiffrer les Données Client et les Données des Services Professionnels transmises via des réseaux publics. - Microsoft restreint l'accès aux Données Client et aux Données des Services Professionnels stockées sur des supports sortant de ses locaux. Journalisation des Événements. Microsoft consigne ou permet au Client de consigner, les accès et les utilisations des systèmes informatiques contenant des Données Client ou des Données des Services Professionnels, en enregistrant les identifiants d'accès, leurs heures et dates d'accès, les autorisations/refus d'accès et les activités effectuées.
Contrôle des accès	Politique de Gestion des Accès. Microsoft conserve un registre des droits de gestion de la sécurité de chaque individu ayant accès aux Données Client et aux Données des Services Professionnels. Autorisation d'Accès - Microsoft conserve et actualise un registre des membres du personnel autorisés à accéder aux systèmes renfermant des Données Client ou des Données des Services Professionnels. - Microsoft désactive les droits d'accès inutilisés durant au moins six (6) mois. - Microsoft identifie les membres de son personnel susceptibles d'accorder, de modifier ou d'annuler une autorisation d'accès aux données et ressources. - Lorsque plusieurs de ses membres sont autorisés à accéder à des systèmes contenant des Données Client ou des Données des Services Professionnels, Microsoft veille à ce que chacun utilise un mot de passe/identifiant qui lui est propre. Droits d'Accès Minimum - Les techniciens de support peuvent accéder aux Données Client et aux Données des Services Professionnels uniquement lorsque cet accès est justifié. - Microsoft restreint l'accès aux Données Client et aux Données des Services Professionnels aux seuls membres dont le travail l'exige. Intégrité et Confidentialité - Microsoft enjoint les membres de son personnel à désactiver leurs sessions administrateur lorsqu'ils quittent les locaux sous le contrôle de Microsoft ou s'éloignent de leur ordinateur. - Microsoft utilise une technologie de stockage des mots de passe qui les rend inintelligibles tant qu'ils sont en vigueur. Authentification - Microsoft applique des procédures conformes aux normes de l'industrie pour identifier et authentifier les utilisateurs tentant d'accéder à ses systèmes informatiques. - Concernant les mécanismes d'authentification fondés sur les mots de passe, Microsoft exige le renouvellement régulier des mots de passe. - Concernant les mécanismes d'authentification fondés sur les mots de passe, Microsoft exige que les mots de passe comportent huit (8) caractères au minimum.

Domaine	Pratiques
	- Microsoft s'assure que les identifiants désactivés ou expirés ne sont pas réaffectés à d'autres individus. - Microsoft contrôle, ou permet au Client de contrôler, les tentatives répétées d'accès aux systèmes d'information avec un mot de passe non valable. - Microsoft applique des procédures conformes aux normes de l'industrie pour désactiver les mots de passe corrompus ou involontairement divulgués. - Microsoft applique des procédures conformes aux normes de l'industrie de protection de mots de passe standard, notamment pour préserver la confidentialité et l'intégrité des mots de passe lors de leur attribution et distribution, puis de leur stockage. Conception du Réseau. Microsoft a mis en place des mesures de contrôle pour éviter que des individus accèdent à des Données Client et des Données des Services Professionnels au moyen de droits d'accès usurpés.
Gestion des incidents de sécurité informatique	Procédure de Gestion des Incidents - Microsoft conserve un registre des failles de sécurité décrivant les failles, la période concernée, les conséquences des failles, l'identité de l'auteur du signalement et celle du destinataire du signalement, ainsi que la procédure de récupération de données appliquée. - Pour chaque faille de sécurité qui est un Incident de Sécurité, une notification sera envoyée par Microsoft (comme indiqué dans la clause « Notification des Incidents de Sécurité » ci-dessus) dans les meilleurs délais et, dans tous les cas, dans les soixante-douze (72) heures. - Microsoft tient, ou permet au Client de tenir, un registre des divulgations de Données Client et de Données des Services Professionnels, notamment des données divulguées, des destinataires desdites données et du moment des divulgations. Surveillance des Services. Les agents de sécurité de Microsoft vérifient les journaux au moins tous les six (6) mois afin de proposer des méthodes de résolution des incidents, au besoin.
Gestion de la continuité des opérations	- Microsoft dispose de plans de secours et d'urgence pour les locaux qui contiennent des systèmes informatiques traitant des Données Client et des Données des Services Professionnels. - Les systèmes de stockage redondants et les procédures de récupération de données de Microsoft sont conçus pour restaurer les Données Client et les Données des Services Professionnels dans l'état d'origine ou précédant leur perte ou destruction.

III - Descriptions des mesures techniques et organisationnelles mises en place par le sous-traitant ultérieur POSTMARK (extrait du DPA conclu entre KYDOC et POSTMARK [version traduite]) :

- L'importateur de données et, lors de la transmission, également l'exportateur de données mettent en oeuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité des données, y compris la protection contre une violation de la sécurité entraînant une destruction, une perte, une altération, une divulgation non autorisée ou un accès non autorisé à ces données (ci-après « violation de données personnelles »).

Lors de l'évaluation du niveau de sécurité approprié, les Parties tiendront dûment compte de l'état de la technique, des coûts de mise en oeuvre, de la nature, de la portée, du contexte et de la ou des finalités du traitement ainsi que des risques liés au traitement pour les personnes concernées. . Les Parties envisageront notamment de recourir au cryptage ou à la pseudonymisation, y compris lors de la transmission, lorsque la finalité du traitement peut être remplie de cette manière. En cas de pseudonymisation, les informations supplémentaires permettant d'attribuer les données personnelles à une personne concernée spécifique restent, dans la mesure du possible, sous le contrôle exclusif de l'exportateur de données. Pour se conformer à ses obligations en vertu du présent paragraphe, l'importateur de données met au moins en oeuvre les mesures techniques et organisationnelles spécifiées à l'annexe II. L'importateur de données effectue des contrôles réguliers pour s'assurer que ces mesures continuent d'assurer un niveau de sécurité approprié.

- L'importateur de données n'accorde l'accès aux données personnelles aux membres de son personnel que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Il garantit que les personnes autorisées à traiter les données personnelles se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale appropriée de confidentialité.
- L'importateur de données coopère avec l'exportateur de données et l'assiste pour lui permettre de se conformer à ses obligations en vertu du règlement (UE) 2016/679, en particulier pour informer l'autorité de contrôle compétente et les personnes concernées, en tenant compte de la nature des traitement et les informations dont dispose l'importateur de données

IV - Descriptions des mesures techniques et organisationnelles mises en place par le sous-traitant ultérieur UNIVERSIGN :

La politique de confidentialité des données gérées par Universign est disponible en ligne à l'adresse <https://www.universign.com/fr/politique-protection-donnees>.

ANNEXE IV : LISTE DE SOUS-TRAITANTS ULTERIEURS

NOM	ADRESSE	DESCRIPTION DU TRAITEMENT
Microsoft	Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown Dublin 18 Ireland	Utilisation de la suite Microsoft 365 (Saas), Azure DevOps pour contrôle de code source et gestion de projets (Saas), hébergement « cloud » de l'application Kydoc
Postmark	1 N Dearborn St, Chicago, IL 60602, États-Unis	Envoi de courriels (Saas)
Universign	7 Rue du Faubourg Poissonnière, 75009 Paris	Signature électronique certifiée (Saas)