

**ACCORD DE PROTECTION DES DONNÉES ENTRE RESPONSABLE DE TRAITEMENT ET
SOUS-TRAITANT**

Version du 03/09/2025

ENTRE LES SOUSSIGNÉS

IOGA, société par actions simplifiée au capital de 30 000 € dont le siège social est situé 149 rue Oberkampf 75011 PARIS, immatriculée au registre du commerce et des sociétés sous le numéro 852 548 098, représentée par Alban Peleszko agissant en sa qualité de Président ayant tous pouvoirs à l'effet des présentes,

Ci-après “le Sous-Traitant” ou “le Prestataire” d’une part

Et

La société _____ au capital de _____ €, immatriculée au R.C.S. _____ sous le numéro _____, dont le siège social est sis _____, représentée par M _____, ayant tous pouvoirs à l'effet des présentes,

Ci-après “le Responsable de Traitement”, ou “le Client” d’autre part,

le Responsable de Traitement et le Sous-Traitant étant ci-après nommés “les Parties” et individuellement “une Partie”.

Si les champs ci-dessus ne sont pas renseignés, ils sont réputés être les champs équivalents du dernier bon de commande, contrat ou document similaire engageant les Parties.

Table des matières

1 EXPOSÉ	3
2 DÉFINITIONS	3
3 OBJET	3
4 DURÉE	3
5 OBLIGATIONS DU SOUS-TRAITANT VIS-À-VIS DU RESPONSABLE DE TRAITEMENT	3
5.1 Finalités	3
5.2 Instructions	4
5.3 Confidentialité	4
5.4 Privacy by design	4
5.5 Sous-traitance ultérieure	4
5.6 Transferts de données vers des pays tiers	5
5.7 Information des personnes concernées	5
5.8 Exercice des droits des personnes	5
5.9 Violations de données à caractère personnel	5
5.9.1 Violation de données en rapport avec des données traitées par le Client	6
5.9.2 Violation de données en rapport avec des données traitées par le Sous-traitant	6
5.10 Assistance au Responsable de Traitement	6
5.11 Mesures techniques et organisationnelles	7
5.12 Sort des Données	7
5.13 Interlocuteur privilégié	7
5.14 Registre des catégories de traitement	8
5.15 Documentation et conformité	8
6 OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS À VIS DU SOUS-TRAITANT	9
6.1 Données	9
6.2 Instructions	9
6.3 Conformité au RGPD	9
6.4 Supervision	9
7 Clauses Contractuelles Types	9
8 DISPOSITIONS GÉNÉRALES	9
ANNEXE 1 - DESCRIPTION DES TRAITEMENTS CONFIÉS AU SOUS-TRAITANT	11
ANNEXE 2 - DÉTAILS DES TRAITEMENTS & SOUS-TRAITANTS ULTÉRIEURS	11
ANNEXE 3 - Clauses Contractuelles Types	13
Annexe I aux clauses contractuelles types	14
Annexe II aux clauses contractuelles types	15
Annexe III aux clauses contractuelles types	16

1 EXPOSÉ

Les Parties ont conclu un contrat de prestation de services (ici appelé « contrat principal ») et qualifié de « sous-traitance » au sens du RGPD en date du contrat principal.

Le contrat principal auquel se rattache le présent accord peut procéder indifféremment d'une convention écrite, d'un bon de commande, de conditions particulières et/ou générales acceptées ou encore d'une offre et d'une acceptation sous quelque forme.

Il conduit le Client, Responsable du Traitement, à confier des données à caractère personnel pour l'exécution des prestations confiées au Sous-traitant et résumées en annexe (annexe 1).

En additif à ce contrat et pour une exécution conforme de la sous-traitance avec la réglementation européenne et en particulier le Règlement Général de la Protection des Données (UE) 2016/679 entré en vigueur en date du 25 mai 2018 (ci-après « le RGPD »), les parties conviennent des clauses contractuelles du présent accord qui s'appliqueront à leur relation de sous-traitance et le cas échéant à toute sous-traitance ultérieure. Elles intègrent les dispositions du RGPD et viennent compléter le contrat principal sur les points évoqués ci-dessous.

2 DÉFINITIONS

Pour la bonne compréhension des présentes clauses s'appliquant à toutes relations de prestations de services (désignée « sous-traitance ») portant sur des données à caractère personnel, les termes employés dans ces clauses (données, responsable de traitement, Sous-traitant, etc.) auront de convention expresse, la définition que le RGPD (notamment son article 4) leur attribue.

Pour les besoins du présent accord, le Client sera désigné aux présentes sous les termes « Responsable de Traitement » ou « Client », même s'il agit lui-même en tant que sous-traitant pour le compte d'un responsable du traitement tiers.

3 OBJET

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018, ci-après désigné « le règlement européen sur la protection des données » (ou « RGPD » ou « GDPR »).

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable de traitement, les opérations de traitement de données à caractère personnel qui lui seront confiées, décrites en **annexe 1**, afin de garantir aux personnes concernées et au Responsable de Traitement, la sécurité, la disponibilité, la confidentialité et la protection, et pour l'exécution desquelles le Responsable de Traitement met à la disposition du Sous-traitant les informations nécessaires et instructions particulières s'il y a lieu, listées à l'**annexe 1**.

4 DURÉE

Les présentes clauses ont vocation à s'appliquer à compter de la signature du présent accord pendant toute la durée du contrat principal. Les présentes clauses prennent fin de plein droit à la fin du contrat principal, sauf les dispositions, notamment de confidentialité, qui survivent à la fin du contrat principal.

Lorsque le contrat principal a pris effet avant la signature des présentes clauses, le Sous-traitant s'engage à prendre toutes les mesures nécessaires pour respecter les présentes clauses, s'il ne l'a pas déjà fait à son initiative, par anticipation de la signature des présentes, pour intégration dans son organisation, des dispositions du RGPD.

5 OBLIGATIONS DU SOUS-TRAITANT VIS-À-VIS DU RESPONSABLE DE TRAITEMENT

Les obligations du Sous-traitant relativement aux traitements qu'il effectue pour le compte du Responsable de traitement sont décrites ci-après.

5.1 Finalités

Le Sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe 1 « Description des traitements », sauf instruction complémentaire du Client.

5.2 Instructions

Le Sous-traitant ne traite les données à caractère personnel que sur instruction documentée du Client, 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 Client 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 Client pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées. Le Sous-traitant et le Client conviennent que ces instructions sont notamment fournies par le Client via l'utilisation ou le paramétrage des services du Sous-traitant utilisés par le Client et que la traçabilité de cette utilisation ou de ce paramétrage constitue une documentation valide desdites instructions. Les Parties conviennent expressément de ce que le DPA, ainsi que le Contrat Principal, constituent des instructions documentées du Client au sens du paragraphe précédent.

Au travers du présent accord, le Responsable du traitement donne instruction au Sous-traitant de traiter les données à caractère personnel du Responsable du traitement afin de permettre l'exécution du contrat principal régi par le contrat principal ou les Conditions Générales (de Vente, de Service, d'Utilisation) le cas échéant.

Par ailleurs, 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 ou de toute législation applicable, sans pour autant être tenu d'auditer systématiquement l'ensemble des informations et des documents fournis par le Responsable du traitement dans le cadre du Contrat Principal.

5.3 Confidentialité

Garantir la confidentialité des données à caractère personnel traitées dans le cadre du contrat principal.

Veiller à ce que toutes personnes autorisées à traiter les données à caractère personnel en vertu du contrat principal :

- S'engagent contractuellement à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- Reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

5.4 Privacy by design

Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et par défaut.

5.5 Sous-traitance ultérieure

- a. Autorisation écrite générale : Le recrutement d'un sous-traitant ultérieur par le Sous-traitant se fait avec l'autorisation générale du Client (respectivement du Responsable de traitement), qui en sera informé par tout moyen convenu entre les Parties. Dans le cas général, le Client (respectivement le Responsable de traitement) recevra la notification d'ajout/suppression ou modification du/des sous-traitants ultérieurs au plus tard 10 jours avant la mise en œuvre de celle-ci et pourra émettre des objections jusqu'à 5 jours avant le recours effectif aux services dudit/desdits sous-traitants. Si la situation le justifie, notamment en raison de considérations liées

à la protection ou à la sécurité des données, le délai minimal de prévenance est porté à 5 jours pour l'envoi de la notification et le Client (respectivement le Responsable du traitement) pourra émettre des objections jusqu'à 3 jours avant le recours effectif aux services dudit/desdits sous-traitants. Au-delà de cette période, sans instruction du Client (respectivement du Responsable de traitement), le sous-traitant ultérieur sera réputé être autorisé par le Client (respectivement le Responsable de traitement). Le Sous-traitant fournit au Client les informations nécessaires pour lui permettre d'exercer son droit d'opposition et les éventuels arguments justifiant le délai raccourci, le cas échéant.

- 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 chaque 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 Client, 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 Client, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le Sous-traitant informe le Responsable de traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
- e. Le Responsable du traitement reconnaît et accepte expressément la liste des sous-traitants ultérieurs figurant à l'annexe 2 du présent accord.

Dans le cas où il existerait par ailleurs une relation de sous-traitance, directe ou indirecte, entre le Responsable de traitement et un des sous-traitants ultérieurs utilisés par le Sous-traitant pour l'exécution des traitements sous-traités objets des présentes, les termes des relations contractuelles entre le Responsable de traitement et le Sous-traitant ne s'appliqueraient nullement aux traitements ainsi sous-traités par le Responsable de traitement auprès dudit sous-traitant ultérieur. La responsabilité du Sous-traitant ne peut nullement être engagée au titre des traitements sous-traités directement par le Responsable de traitement auprès d'un sous-traitant ultérieur lorsque ces traitements ne sont pas sous-traités par le Sous-traitant pour le compte du Responsable de traitement dans le cadre de la fourniture des Services objets des présentes.

5.6 Transferts de données vers des pays tiers

Dans le cas où les traitements impliquent des transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, le Sous-traitant vérifie l'existence et / ou établit les garanties appropriées notamment en vertu de l'article 46 du RGPD, en particulier l'exécution des clauses contractuelles types de la commission européenne (article 46, § 2, alinéa d du RGPD) disponible via ce lien :

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32021D0914&from=FR>

Dans un tel cas, lesdites clauses contractuelles types sont réputées être incorporées par référence au présent accord, avec les options et adaptations précisées en annexe.

5.7 Information des personnes concernées

Il appartient au Responsable de Traitement de fournir l'information qui est due, conformément à la législation, aux personnes concernées par les opérations de traitement, au moment de la collecte des données ou ultérieurement, de préférence avant la mise en œuvre du traitement sous-traité.

L'assistance due par le Sous-traitant au Responsable de Traitement est décrite dans la section 5.9 du présent accord.

Le Sous-traitant doit ainsi transmettre au Responsable de Traitement, sur demande, toute information relative aux traitements qu'il effectue pour le compte du Responsable de Traitement et qui doit être apportée aux personnes concernées, notamment en ce qui concerne les transferts de données dans des pays extérieurs à l'UE et les mesures techniques et organisationnelles par lui prises pour le traitement conforme des données. Si le Sous-traitant constate que les informations apportées peuvent ne pas être suffisantes à l'information des personnes, le Sous-traitant doit, avant toute intervention de sa part, renseigner le Responsable de Traitement des informations complémentaires spécifiques à l'objet du traitement devant être apportées aux personnes dont les données sont traitées.

5.8 Exercice des droits des personnes

L'assistance due par le Sous-traitant au Responsable de Traitement est décrite dans la clause 5.10 ci-dessous.

Dans la mesure du possible, le Sous-traitant doit aider le Responsable de Traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées, notamment droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées par le traitement des données à caractère personnel exercent auprès du Sous-traitant des demandes d'exercice de leurs droits, le Sous-traitant doit adresser ces demandes sans délai après leur réception, au moyen d'un courrier électronique adressé au Responsable de Traitement (à son DPO s'il en désigné un ou, à défaut, à un point de contact idoine et prédéfini entre les Parties), lui apportant toutes informations utiles concernant le traitement effectué par le Sous-traitant, pour permettre au Responsable de Traitement d'y répondre. L'adresse de courriel que le Sous-traitant doit utiliser est précisée en Annexe du présent accord.

Le Responsable de traitement autorise le Sous-traitant à répondre à des demandes de personnes concernées, avant toute notification au Responsable de traitement, uniquement afin de déterminer si la demande concerne des données personnelles traitées par le Sous-traitant pour le compte du Responsable de traitement.

Si l'adresse électronique de contact indiquée à l'annexe 2 n'est pas complétée, elle est réputée être l'adresse électronique publique du DPO du Responsable du traitement, l'adresse spécifiée dans l'annexe appropriée du présent accord ou, en l'absence d'une telle adresse électronique, l'adresse électronique de contact spécifiée dans le bon de commande, le contrat ou le document similaire le plus récent engageant les parties.

5.9 Violations de données à caractère personnel

En cas de violation de données à caractère personnel, le Sous-traitant coopère avec le Client 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.

5.9.1 Violation de données en rapport avec des données traitées par le Client

En cas de violation de données à caractère personnel en rapport avec des données traitées par le Client lorsque les traitements en question sont corrélés aux services rendus par le Sous-traitant au Responsable de traitement, le Sous-traitant prête assistance au Client :

- 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 Client et le responsable du traitement en ont 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 ou à l'article 34, paragraphe 3, du règlement (UE) 2018/1725, selon ce qui s'applique, doivent figurer dans la notification du Client, 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 coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel;
 - 3 les conséquences probables de la violation de données à caractère personnel;
 - 4 les mesures prises ou les mesures que le Client 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 ou à l'article 35 du règlement (UE) 2018/1725, selon ce qui s'applique, 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.

5.9.2 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 pour le compte du Responsable de traitement, celui-ci en informe le Client 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 le cas échéant en annexe aux présentes tous les autres éléments que le Sous-traitant doit communiquer lorsqu'il prête assistance au Client aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679/ ou des articles 34 et 35 du règlement (UE) 2018/1725, selon ce qui s'applique.

En pareil cas, le Sous-traitant devra notifier le Client de la violation de données au plus tard dans un délai de 48 h à compter du moment où il en aura connaissance.

5.10 Assistance au Responsable de Traitement

- a) Le Sous-traitant informe sans délai le Client 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 Client ne l'y ait autorisé.
- b) Le Sous-traitant prête assistance au Client 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 Client.

- c) Outre l'obligation incombant au Sous-traitant d'assister le Client en vertu de la clause 5.10, point b), le Sous-traitant aide en outre le Client 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 Client et/ou le responsable de 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 Client 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 ou aux articles 33, 36 à 38 du règlement (UE) 2018/1725, selon ce qui s'applique.
- d) Les Parties définissent à l'annexe 3 les mesures techniques et organisationnelles appropriées par lesquelles le Sous-traitant est tenu de prêter assistance au Client dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

5.11 Mesures techniques et organisationnelles

Les obligations du Sous-traitant en ce qui concerne les mesures techniques et organisationnelles à mettre en œuvre dans le cadre des traitements qu'il effectue pour le compte du Responsable de traitement sont régies par les dispositions suivantes :

- 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 traitées par le Sous-traitant pour le compte du Client dans le cadre du Contrat principal. Figure parmi ces mesures la protection desdites 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 selon les termes du Contrat principal 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 lesdites données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

5.12 Sort des Données

À la suite de la résiliation du contrat, le Sous-traitant supprime, selon le choix du Client, toutes les données à caractère personnel traitées pour le compte du Responsable du traitement et certifie auprès du Client qu'il a procédé à cette suppression dans le mois suivant cette demande de suppression, ou selon l'instruction reçue, dans ce même délai, renvoie toutes les données à caractère personnel au Client 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.

5.13 Interlocuteur privilégié

Désigner un interlocuteur privilégié : Le Sous-traitant doit communiquer au Responsable de Traitement le nom et les coordonnées de la personne ou du service en charge compétent pour ce qui concerne la protection des données à caractère personnel. Ce peut être un délégué à la protection des données (DPO). Tout changement ultérieur relativement à ce point de contact doit être notifié dans les plus brefs délais au Responsable de Traitement. L'interlocuteur privilégié désigné par le Sous-traitant est contactable selon les modalités précisées en annexe.

5.14 Registre des catégories de traitement

Le Sous-traitant déclare être en capacité de produire, sur simple demande du Responsable de Traitement ou de toute autorité compétente, un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de Traitement comprenant au moins :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels Sous-traitants et, le cas échéant, des délégués à la protection des données (le sien, celui du Responsable de Traitement et des éventuels Sous-traitants ultérieurs) ;
- Les catégories de traitements effectués pour le compte du Responsable du Traitement,
- Les destinataires des données,
- Les éventuels transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale (et, dans le cas des transferts visés à l'article 49, § 1, 2^{ème} alinéa du RGPD, les documents attestant de l'existence de garanties appropriées),
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins, les mesures décrites au point [5.10](#) ci-dessus.

5.15 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 Client, 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 et de ses sous-traitants ultérieurs.
- 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.

Le Sous-traitant devra fournir au Responsable de Traitement, à sa demande, les documents relatifs aux mesures techniques et organisationnelles mises en œuvre afin de garantir un niveau de sécurité approprié, ainsi que les autres informations nécessaires pour démontrer le respect par le Fournisseur des obligations lui incombant aux termes du présent Contrat et en vertu de la Législation relative à la Protection des Données.

Le Responsable du Traitement et l'autorité de contrôle compétente en vertu de la Législation relative à la Protection des Données seront en droit de procéder à des contrôles, y compris des inspections et des évaluations sur site relatives aux Données à Caractère Personnel traitées, aux systèmes et équipements

utilisés pour ce traitement, aux mesures techniques et organisationnelles mises en œuvre (y compris les règles de sécurité et similaires) et aux sous-traitants du Sous-traitant.

Le Responsable du traitement pourra procéder à de tels contrôles une (1) fois, une journée par an, à condition d'observer un préavis d'au moins quatre semaines. Si le Responsable de Traitement confie à un vérificateur externe le soin de procéder aux contrôles en question, ce vérificateur sera soumis à une obligation de confidentialité. Le Sous-traitant disposera de la faculté de s'opposer à la désignation d'un auditeur tiers spécifique si, pour des raisons impérieuses tenant à sa situation spécifique (par exemple si l'auditeur tiers est un concurrent du Sous-traitant), la réalisation de l'audit par cet auditeur tiers présente manifestement un risque de lui causer un dommage. En aucun cas l'exercice de la faculté susmentionnée ne saurait avoir pour objet ou pour effet d'empêcher toute réalisation de l'audit par ou pour le compte du Client.

6 OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS À VIS DU SOUS-TRAITANT

Le Responsable de traitement s'engage à :

6.1 Données

Fournir au Sous-traitant, en conformité avec le RGPD, les données appelées à être traitées et/ou les moyens et autorisations de collecter et de traiter lesdites données en application du contrat principal et du présent accord.

6.2 Instructions

Fournir toute instruction utile et documentée concernant le traitement des données par le Sous-traitant selon les seuls termes du Contrat Principal. En particulier, l'utilisation ou le paramétrage de la Solution constituent des instructions fournies par le Responsable de traitement au Sous-traitant.

6.3 Conformité au RGPD

Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD lui incombant, et notamment à l'information ou au consentement des personnes lorsque celui-ci est nécessaire au traitement mis en œuvre, et à la remontée au Sous-traitant des oppositions et retraits de consentement.

6.4 Supervision

Superviser le traitement, réaliser les audits et les inspections auprès du Sous-traitant et en tous lieux où se trouvent mis en œuvre les traitements.

7 Clauses Contractuelles Types

Si le Sous-traitant est situé sur le sol de l'espace économique européen, les clauses contractuelles types mentionnées en annexe de la Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les Sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil sont incorporées au présent accord par référence. Le texte complet est disponible via le lien suivant :

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0018.01.FRA

Les adaptations et options requises, quand elles ne sont pas directement incluses dans le présent accord, y sont présentées en annexes.

En cas de contradiction entre les dispositions du présent accord et celles desdites clauses contractuelles types, ce sont les dispositions des clauses contractuelles types qui prévalent.

8 DISPOSITIONS GÉNÉRALES

Le présent accord complète le Contrat principal relatif à la prestation de services confiée au Sous-traitant par le Client. Il annule et remplace toute clause contraire ou contradictoire du Contrat principal auquel il se rattache.

Toutes autres clauses non affectées par le présent accord, subsistent, à l'exception toutefois des clauses limitatives ou exonératoires de la responsabilité du Responsable du traitement pouvant avoir été stipulées par le Contrat principal ou dans tout autre document à valeur contractuelle ou légale, qui se trouvent en tous les cas, privées d'effet pour le cas de manquement à la protection des données à caractère personnel.

En matière de protection des Données à caractère personnel, le Sous-Traitant ne peut être tenu responsable que des dommages directs causés par un Traitement pour lequel il n'a pas respecté ses obligations au regard des lois sur la protection des données, ou s'il n'a pas respecté ses obligations au regard des lois sur la protection des données concernant les sous-traitants ultérieurs en charge des données, ou encore pour lequel il a agi contrairement aux instructions légales du Client ou en violation des accords entre les Parties (Contrat Principal, présent Accord, etc.). Dans de tels cas, les éventuelles dispositions du Contrat Principal relatives à la responsabilité du Sous-Traitant s'appliquent en ce qui concerne les Traitements de Données à caractère personnel.

Le présent accord ne peut être modifié par l'une des Parties que par voie d'avenant dûment signé par les Parties.

Dans l'hypothèse où des clauses types réglementées seraient adoptées, il est entendu que les présentes clauses seront remplacées par les clauses type contraires ou contradictoires, qui s'y substitueraient.

Tout litige afférant à la conclusion, l'exécution ou l'inexécution, l'interprétation des règles de protection des données sera soumis à la loi du pays du Sous-traitant.

Fait à _____ le _____

Pour le Sous-traitant

Pour le Responsable de traitement

Si les champs ci-dessus ne sont pas remplis, ils sont réputés être les champs équivalents du dernier bon de commande, contrat ou document similaire engageant les parties.

ANNEXE 1 - DESCRIPTION DES TRAITEMENTS CONFIEES AU SOUS-TRAITANT

Service(s) ou prestation(s) fourni(s) en application du contrat principal :

- Fourniture d'une plateforme SaaS (Software as a Service) de digitalisation des processus de transfert et de capitalisation des connaissances, notamment par le biais d'interviews vidéo.

Nature des opérations réalisées sur les données :

- Collecte
- Enregistrement
- Stockage
- Utilisation aux fins de rendre les services ou prestations ci-dessus
- Transfert
- Restitution
- Suppression

Finalité(s) du traitement :

- Digitalisation des processus de transfert et de capitalisation des connaissances, notamment par le biais d'interviews vidéo
- Retranscription textuelle desdits interviews
- Gestion et optimisation du suivi des processus de transfert et de capitalisation des connaissances

Données à caractère personnel susceptibles d'être traitées :

- État civil, identité, données d'identification, images... : Nom, prénom, numéro de téléphone professionnel, adresse postale professionnelle, adresse email professionnelle de la personne concernée, fonction, condensat asymétrique du mot de passe d'accès au service IOGA
- Données de connexion (adresse IP, logs, etc.) : Adresse IP de connexion, historique de navigation, détails techniques des terminaux, langue du navigateur
- Toute catégorie de données contenues dans un document versé au sein de l'application ou une vidéo enregistrée par le Client ou une personne autorisée par le Client à utiliser l'application.

Catégories de personnes concernées :

- Employés ou collaborateurs du Client
- Professionnels invités à collaborer au sein de la plateforme par une personne des catégories précédentes
- Toute catégorie de personne dont des données la concernant sont contenues dans une vidéo enregistrée par ou pour le Client, dans un document versé au sein de l'application par le Client ou une personne autorisée par le Client à utiliser l'application.

Informations nécessaires suivantes fournies ou à fournir par le Responsable de Traitement pour l'exécution du service :

- Coordonnées des utilisateurs de la solution, notamment adresse email desdits utilisateurs.
- Coordonnées des utilisateurs administrateurs de la solution qui pourront créer des utilisateurs de la solution, notamment adresse email desdits administrateurs.

Instructions particulières du responsable de traitement :

Compléments, s'il y a lieu :

Le Sous-traitant met à la disposition du Responsable de traitement les informations suivantes

:

- Notice d'information des personnes concernées
- Mentions légales sur formulaire
- Modalité d'information des personnes concernées

ANNEXE 2 - DÉTAILS DES TRAITEMENTS & SOUS-TRAITANTS ULTÉRIEURS

DÉTAILS DES TRAITEMENTS ET DÉSIGNATION DE SOUS-TRAITANTS ULTÉRIEURS PAR LE SOUS-TRAITANT

Sous-traitants ultérieurs et fournisseurs	Description	Adresse	Pays de traitement de données	Détails, commentaires, garanties
Amazon Web Service	Fournisseurs de stockage en ligne, fournisseur de solution PaaS (Platform as a Service)	38 avenue John F. Kennedy, L-1855 Luxembourg	UE (France)	https://aws.amazon.com/compliance/gdpr-center/ https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf (partie intégrant des conditions de service d'AWS) Conformité DPF Modèle de responsabilité partagée : https://aws.amazon.com/fr/compliance/shared-responsibility-model/ Certification ISO : https://aws.amazon.com/fr/compliance/iso-certified/
Juby	Expertise architecture et maintenance de la plateforme	27, avenue Pablo Picasso 93400 Saint-Ouen-sur-Seine	France	DPA et Clauses Contractuelles Types
Officienne	Expertise architecture et maintenance de la plateforme	47, Bd de Sébastopol 75001 Paris	France	DPA et Clauses Contractuelles Types
Studio Millebruits	Aide à la réalisation de vidéo	10, rue Simon 51100 Reims	France	DPA et Clauses Contractuelles Types
Microsoft Azure	Fournisseur de services Cloud Services d'IA	37 quai du Président Roosevelt 92130 Issy les Moulineaux	Europe (Suisse)	Certifié ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP et ENS DPA : https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA Informations privacy et sécurité : https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy Conformité : https://azure.microsoft.com/fr-fr/explore/

				trusted-cloud/compliance Certifications : https://learn.microsoft.com/fr-fr/azure/compliance/ Code de Conduite approuvé : https://learn.microsoft.com/fr-fr/azure/compliance/offerings/offering-eu-cloud-coc
SysStreaming	Cabinet DPO externalisé	34, rue de l'orme sec 94240 L'Haÿ les Roses	France	DPA et Clauses Contractuelles Types

Note :

Nous ne sommes généralement pas toujours en mesure de donner les adresses physiques exactes où les données sont traitées en raison de la façon dont les fournisseurs cloud fonctionnent au niveau technique. Ce mode de fonctionnement est basé sur l'architecture même des fournisseurs. Un fournisseur Cloud possède généralement des « régions » dans le monde entier. Au sein de ces régions, il existe le concept de « zones de disponibilité ». Un nœud hébergé par un fournisseur Cloud est situé dans une ou plusieurs zones de disponibilité d'une région donnée. Indépendamment du choix du propriétaire du nœud de répliquer les données à l'intérieur d'une région ou entre les régions, le fournisseur Cloud lui-même peut répliquer les données à l'intérieur de la région vers d'autres zones de disponibilité, notamment pour assurer la haute-disponibilité via redondance multi-sites. Il en résulte que les données traitées par le biais d'un fournisseur Cloud existent en général dans plusieurs installations au sein d'une région donnée. En outre, pour des raisons de sécurité, les fournisseurs Cloud n'autorisent généralement pas la communication de l'emplacement spécifique des bâtiments de leurs centres de données ou des installations associées.

Ainsi, loga ne peut s'engager sur une localisation des traitements qu'au niveau de la région Europe. Les mentions de pays ne sont données dans le tableau ci-dessus qu'à titre indicatif et peuvent changer.

ANNEXE 3 - Clauses Contractuelles Types

Les clauses contractuelles types mentionnées en annexe de la Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil s'appliquent au présent accord, avec les adaptations, les options et les détails suivants :

Clause 1 : Option 1

Clause 5 optionnelle : la clause s'applique

Clause 7.7.a : Option 2. Durée : 10 jours calendaires.

Clause 8.c.4 : Option 1

Clause 9.1.c : Option 1

Clause 9.2.c : Option 1

Contact du DPO du Sous-traitant, du service ou de la personne en charge des questions relatives à la protection des données : dpo@ioga.fr

Contact du DPO du Responsable du traitement, du service ou de la personne en charge des questions relatives à la protection des données : XXXXXX@YYY.ZZZ

Contact du Responsable de traitement à utiliser pour transmettre les demandes d'exercices de droits reçues par le Sous-traitant : XXXXXXXXXXXX@YYY.ZZZ

Contact du responsable de traitement à utiliser pour notifier des violations de données constatées par le Sous-traitant : [adresse e-mail du RSSI / du DPO / autre - à préciser le cas échéant]

Dans le cadre des transferts de données à caractère personnel depuis ou vers des pays tiers, effectués dans le cadre du contrat entre le Sous-Traitant et le Responsable de Traitement et lorsque le traitement implique des transferts de données à caractère personnel avec un pays tiers jugé non-adéquat par la Commission européenne

Annexe à la DÉCISION D'EXÉCUTION (UE) 2021/914 DE LA COMMISSION du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil

Les modules suivants sont ceux à prendre en compte

MODULE DEUX : Transfert du responsable de traitement à sous-traitant

MODULE TROIS : Transfert de sous-traitant à sous-traitant

MODULE QUATRE : Transfert du sous-traitant au responsable de traitement

Les Clauses Contractuelles Types sont exécutées avec les options et les choix suivants :

Clause 7 - Optionnel : la clause ne s'applique pas.

Clause 9 - Module DEUX, Module TROIS et Module QUATRE: OPTION 2, délai = 10 jours calendaires

Clause 11 - Paragraphe (a) : L'OPTION ne s'applique pas

Clause 13 - Module DEUX et Module TROIS - OPTION 1 : État membre dans l'État français.

Clause 17 - Module DEUX et Module TROIS : OPTION 1 - le pays est la France

Clause 17 - Module QUATRE : le pays est la France

Clause 18 - Module DEUX et Module TROIS - Paragraphe (b) : L'État membre est l'État français.

Clause 18 - Module QUATRE : Le pays est la France.

Points de contact

- Contact du Responsable de Traitement à utiliser pour transmettre les demandes d'exercices de droits reçues par le Sous-traitant : voir annexe au Contrat
- Contact du Responsable de Traitement à utiliser pour notifier des violations de données constatées par le Sous-traitant : voir annexe au Contrat
- Contact du Responsable de Traitement à utiliser pour les autres notifications (projet de changement dans la liste des sous-traitants en particulier) : voir annexe au Contrat
- Contact du Sous-traitant à utiliser pour les demandes d'exercices de droits : voir annexe au Contrat
- Contact du Sous-traitant à utiliser pour les notifications : voir annexe au Contrat

Si les adresses ci-dessus ne sont pas renseignées, elles sont réputées être :

- *Pour le Client : l'adresse de courriel publique du DPO du Client ou, s'il n'existe pas de telle adresse publique, l'adresse de courriel de contact de la ou des personne(s) en charge des relations avec le Prestataire pour le compte du Client, ou, à défaut d'autres adresses de courriel de contact, l'adresse de courriel de contact générique du Client, telle que présente sur son site web ou dans tout document approprié*
- *Pour le Sous-traitant : l'adresse de courriel publique du DPO du Sous-traitant ou, s'il n'existe pas de telle adresse publique, l'adresse de courriel de contact de la ou des personne(s) en charge des relations avec le Client pour le compte du Sous-traitant, ou, à défaut d'autres adresses de courriel de contact, l'adresse de courriel de contact générique du Sous-traitant, telle que présente sur son site web ou dans tout document approprié*

Annexe I aux clauses contractuelles types

Liste des parties

Responsable(s) du traitement :

[Identité et coordonnées du ou des responsables du traitement et, le cas échéant, du délégué à la protection des données du responsable du traitement]

1.

Nom, adresse, etc. : Le Responsable de traitement, tel que défini à la première page de l'Accord

Nom, fonction et coordonnées de la personne de contact : se référer à la section "Instructions particulières du responsable de traitement" de l'Annexe 1 du présent Accord.

Signature et date d'adhésion: ...

Sous-traitant(s) :

[Identité et coordonnées du ou des sous-traitants et, le cas échéant, du délégué à la protection des données du sous-traitant]

1.

Nom, adresse, etc. : Le Sous-traitant, tel que défini à la première page de l'Accord

Nom, fonction et coordonnées de la personne de contact : se référer à la section 5.13 du présent Accord

Signature et date d'adhésion:

2.

Nom: ...

Adresse: ...

Nom, fonction et coordonnées de la personne de contact: ...

Signature et date d'adhésion: ...

Si les noms, adresse, fonctions, coordonnées et signatures ne sont pas présentes et les dates d'adhésion ne sont pas précisées, ces éléments sont réputés être ceux du contrat Principal

Annexe II aux clauses contractuelles types

Description du traitement

Catégories de personnes concernées dont les données à caractère personnel sont traitées
Se référer à l'Annexe 1 de l'Accord

Catégories de données à caractère personnel traitées
Se référer à l'Annexe 1 de l'Accord

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.
Aucune donnée sensible n'est traitée dans le cadre de l'Accord ni des relations contractuelles

Nature du traitement
Se référer à l'Annexe 1 de l'Accord

Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement
Se référer à l'Annexe 1 de l'Accord

Durée du traitement
Se référer à l'Annexe 1 de l'Accord

Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement.
Se référer à l'Annexe 1 de l'Accord

Annexe III aux clauses contractuelles types

Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants (y compris toute certification pertinente) visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Mesures de pseudonymisation des données à caractère personnel

- Les utilisateurs sont identifiés au sein de l'application mise à disposition du responsable de Traitement par le Sous-traitant (ci-après "l'Application") par un identifiant interne ne permettant pas leur ré-identification directe.

Mesures de chiffrement des données à caractère personnel

- Les mots de passe des utilisateurs sont stockés sous forme d'empreinte (ou condensat, ou *hash* en anglais, ne permettant pas de déchiffrer la donnée initiale.
- Toutes les données sont chiffrées au repos (avec un algorithme de type AES-256) et en transit (avec TLS, ssh, etc.).

Mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement

- Tous les accès aux données à caractère personnel sont nominatifs et tracés
- Tous les accès à distance destinés à la maintenance ou la configuration des systèmes permettant d'accéder aux données à caractère personnel sont chiffrés (ssh et VPN notamment)
- Tous les comptes permettant d'accéder aux données à caractère personnel sont associés à des habilitations d'accès données sur le principe du besoin d'en connaître.
- Les habilitations sont révoquées dès que le besoin d'en connaître correspondant n'est plus acté
- Les comptes et les habilitations sont revus régulièrement (au moins une fois par an)
- Des analyses de vulnérabilités et de pénétrabilité sont effectuées plusieurs fois par an. Des rapports sont établis comprenant le cas échéant des actions correctives et des recommandations. Un suivi des actions à effectuer est mis en œuvre.
- L'infrastructure est déployée via des processus IaC (*Infrastructure as Code*). Nommément, elle est déployée via processus automatisés.
- Le code est soumis à des revues de code.

Mesures assurant de disposer de moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique

- Tous les stockages sont de type "haute disponibilité".
- Des sondes de disponibilité sont mises en œuvre aux fins de déterminer et d'alerter en cas d'indisponibilité d'un composant nécessaire au traitement des données.
- Des sauvegardes sont effectuées régulièrement
- Des procédures de restauration à partir des sauvegardes ont été élaborées et sont régulièrement testées.

Procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

- Des procédures de restauration à partir des sauvegardes ont été élaborées et sont régulièrement testées.
- Des analyses de vulnérabilités et de pénétrabilité sont effectuées plusieurs fois par an. Des rapports sont établis comprenant le cas échéant des actions correctives et des recommandations. Un suivi des actions à effectuer est mis en œuvre.

- Des analyses de codes sont effectuées
- L'infrastructure est déployée via des processus IaC (*Infrastructure as Code*). Nommément, elle est déployée via processus automatisés.
- Le code est soumis à des revues de code.

Mesures d'identification et d'autorisation de l'utilisateur

- Tous les accès aux données à caractère personnel sont nominatifs et tracés
- Tous les accès à distance destinés à la maintenance ou la configuration des systèmes permettant d'accéder aux données à caractère personnel sont chiffrés (ssh et VPN notamment)
- Tous les comptes permettant d'accéder aux données à caractère personnel sont assortis d'habilitations données sur le principe du besoin d'en connaître.
- Les habilitations sont révoquées dès que le besoin d'en connaître correspondant n'est plus acté
- Les comptes et les habilitations sont revus régulièrement (au moins une fois par an)
- Les comptes génériques ou par défaut sont inhibés

Mesures de protection des données pendant la transmission

- Toutes les données sont chiffrées en transit (avec TLS ou une méthode / un protocole apportant une sécurité similaire, par exemple IMAPS, SMTPS, FTPS, etc.)

Mesures de protection des données pendant le stockage

- Les données des différents clients font l'objet d'une ségrégation logique. Elle s'appuie généralement sur des mécanismes d'association des données à l'identifiant du client pour lequel elles sont traitées, de ségrégation au niveau de la base de données ou encore du système de stockage.
- Toutes les données sont chiffrées au repos avec un algorithme de chiffrement de type AES-256
- Les données sont chiffrées avec des clés propres au client rendant l'accès aux données quasi impossible en dehors de l'application
- Les accès aux fichiers contenant les données, dont fichiers de sauvegardes, sont protégés et réservés aux comptes attribués aux personnes ou aux composants ayant besoin d'en connaître

Mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées

- Les données sont traitées au sein de Data Centers sécurisés et opérés par des acteurs majeurs du secteur donnant toute garantie en la matière et certifiés selon un ou plusieurs des référentiels standards du secteur ISO 27001:2013, SOC 2 Type II, ISO 9001, etc.

Mesures visant à garantir l'enregistrement des événements

- Toutes les actions effectuées sur les données sont tracées

Mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut

- L'infrastructure est déployée via des processus IaC (*Infrastructure as Code*). Nommément, elle est déployée via processus automatisés.
- Le code est soumis à des revues de code.
- Les comptes génériques ou par défaut sont inhibés

Mesures de gouvernance et de gestion de l'informatique interne et de la sécurité informatique

- La direction du Sous-traitant est engagée à fournir les ressources nécessaires à une bonne gestion de l'informatique interne et de la sécurité informatique
- Des points "conformité et sécurité" sont régulièrement faits avec les acteurs concernés (DPO, CTO, COO, etc.)

Mesures visant à garantir la qualité des données

- Journalisation et actions dans l'Application les données sont collectées automatiquement et ne peuvent pas être erronées
- Données personnelles des utilisateurs de l'Application : elles sont modifiables par l'utilisateur de façon à lui permettre une gestion et une mise à jour autonome.
- Des contrôles d'intégrité sont mis en place

Mesures visant à garantir une conservation limitée des données

- Les données peuvent être conservées par défaut durant la relation contractuelle, assortie pour certaines données d'une période de conservation jusqu'aux délais de prescription et de forclusion qui s'appliquent (voir Annexe 1 de l'Accord), mais le responsable de traitement a la possibilité de spécifier une durée moins longue, selon ses besoins, et/ou d'effacer / de modifier certaines données à la demande.

Mesures permettant la portabilité des données et garantissant l'effacement

- Les données peuvent être extraites simplement et sous format standard avec des requêtes de bases de données simples du type (pseudo-code) :
Select * from DataBase where IDClient=<Identifiant du Responsable de Traitement>
- Les données peuvent être effacées simplement avec des requêtes de bases de données simples du type (pseudo-code) :
Delete * from DataBase where IDClient=<Identifiant du Responsable de Traitement>
- Les données de type images / audio peuvent être anonymisées simplement avec des traitements de post-production d'image et de son de type floutage et traitement de fréquences et de timbres sonores

Pour les transferts vers des sous-traitants (ultérieurs), décrire également les mesures techniques et organisationnelles spécifiques que doit prendre le sous-traitant (ultérieur) pour être en mesure de prêter assistance au responsable du traitement.

- Établissement d'accords sur la protection des données avec les sous-traitants ultérieurs dans le cas où de tels accords n'existent pas de façon standardisée dans l'offre du sous-traitant
- Vérification des mesures mentionnées dans les accords de protection des données établis avec les sous-traitants. Vérification de l'exécution des clauses contractuelles types qui s'appliquent. Vérification des droits d'audit qui peuvent être accordés au Responsable de traitement relativement aux traitements effectués par les sous-traitants ultérieurs; Revue des certification des sous-traitants ultérieurs
- Mise à disposition du responsable de traitement desdits accords sur la protection des données

Description des mesures techniques et organisationnelles spécifiques que le sous-traitant doit prendre pour pouvoir prêter assistance au responsable du traitement.

- Fourniture de mentions types d'information qu'il est possible de mettre à disposition des personnes concernées par les traitements mis en oeuvre par le Sous-traitant pour le compte du Responsable de traitement
- Fourniture de rapports d'analyses de vulnérabilité et de pénétrabilité
- Mise en œuvre de procédures de contact et de notification, notamment en cas de demande d'exercice des droits des personnes concernées ou de violation de données.