

## Annexe

### Contrat de sous-traitance des données

La présente annexe au contrat de sous-traitance (ou DPA selon son acronyme anglais) a pour objet de se conformer aux dispositions de l'article 28 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 (ci-après dénommé « Règlement général sur la protection des données » ou « RGPD ») et en vertu des dispositions de la loi organique 3/2018 du 5 décembre relative à la protection des données à caractère personnel et à la garantie des droits numériques (ci-après dénommée « LOPDGDD ») en Espagne, le traitement des données à caractère personnel pour le compte de tiers nécessite la conclusion d'un contrat privé qui établit l'objet, la durée, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement.

Le présent DPA est présenté en annexe aux conditions générales de vente générées avec le bon de commande, de sorte que son acceptation expresse intervient conjointement avec la signature dudit bon de commande et des documents annexés.

Le présent contrat de sous-traitant est constitué des éléments suivants:

#### CLAUSES

##### PREMIER. - DÉFINITIONS - RÔLES DES PARTIES

Les concepts présentés tout au long du contrat suivant, tels que 'données à caractère personnel', 'traitement', 'responsable du traitement', 'sous-traitant', 'pseudonymisation', 'cryptage', etc., doivent être compris conformément à leur définition dans le RGPD, la LOPDGDD et les autorités chargées de la protection des données.

**CLIENT:** la partie qui contracte les services du FOURNISSEUR et qui agira généralement en tant que «Responsable des données à caractère personnel» (le « RESPONSABLE DE TRAITEMENT »). Dans les cas où le CLIENT est un partenaire (distributeur ou collaborateur agréé), celui-ci sera considéré comme le SOUS-TRAITANT, le PRESTATAIRE comme le SOUS-TRAITANT ULTÉRIEUR et ses clients comme les RESPONSABLES (et ainsi de suite s'il y a d'autres parties impliquées). Ci-après, nous ferons exclusivement référence au RESPONSABLE, sans préjudice du fait que le CLIENT puisse être un partenaire.

**PRESTATAIRE:** entreprise du groupe Signaturit qui fournit les services au CLIENT et aux utilisateurs finaux et qui agit généralement en tant que sous-traitant (le « SOUS-TRAITANT »).

**FOURNISSEUR:** entité juridique appartenant au Groupe Signaturit qui fournit les services au CLIENT et qui entretient donc la relation contractuelle principale avec le CLIENT (le 'Prime contractor').

- Le FOURNISSEUR agira en tant que SOUS-TRAITANT s'il fournit également le service final au CLIENT et aux utilisateurs.
- Si le CLIENT a contracté, par l'intermédiaire du FOURNISSEUR, des Services fournis par un autre PRESTATAIRE du Groupe Signaturit, le FOURNISSEUR n'interviendra pas dans le traitement des données à caractère personnel relatives à la prestation du service.

##### DEUXIÈMENT. - OBJET

###### 2.1. Objet du contrat

L'objet du présent contrat est de fixer les conditions générales qui régiront le traitement par le SOUS-TRAITANT (et, le cas échéant, le SOUS-TRAITANT ULTÉRIEUR) des données à caractère personnel contenues dans les systèmes du RESPONSABLE, afin de lui fournir l'un des traitements faisant l'objet du contrat de prestation de services conclu entre les deux parties, aux fins et conformément à ses instructions et au RGPD.

## 2.2. Traitement des données effectué

Le tableau suivant détaille les activités de traitement à réaliser pour le compte du CLIENT, conformément au contenu du contrat de prestation de services signé entre les parties :

SERVICES	VIDSIGNER
Description	Service de signature électronique multicanal
Interessés	A. Utilisateurs de l'application B. Destinataires des processus de signature
Types de données	A. Identification de l'utilisateur et des destinataires : nom, prénom, téléphone, email, NIF ou équivalent, service, fonction, organisation, biométrie du comportement comportemental de la signature manuscrite collectée sur un appareil de type tablette. B. Contact utilisateur : email, téléphone et autres. C. Utilisation du service par l'utilisateur et journal d'audit : PII, URL, navigateur, système d'exploitation, date et géolocalisation facultative. D. Le contenu des documents envoyés par la plateforme. Librement choisi par le responsable du traitement
Traitements	A. Collecte, stockage, stockage et suppression des types de données indiqués B. Requêtes effectuées par l'utilisateur et par les utilisateurs admin C. Exportation des données (annonces) par l'utilisateur et par les utilisateurs admin D. Enregistrement et consultation de l'activité d'utilisation (rapports et audits) E. Préparation de listes et de rapports pour la gestion du service par le PRESTATAIRE F. Envoi d'avis et de communications liés à la fourniture du service G. Collecte des données personnelles (Video ID uniquement).
Fins	Recueillir des preuves électroniques des opérations effectuées avec les documents envoyés par le biais de l'application
Temps de stockage	Les documents seront conservés pendant 60 jours à la disposition du client, avec 30 jours supplémentaires pour le téléchargement.

## 2.3. Obligations et mesures

Le traitement susmentionné sera effectué conformément aux dispositions du RGPD, de la LOPDGDD et de toute autre réglementation applicable en matière de protection des données.

De même, le SOUS-TRAITANT traitera les données des personnes physiques signataires du présent contrat, celles existant entre les parties et celles des personnes physiques travaillant ou utilisant ses services dans le but de gérer la présente relation contractuelle souscrite entre les parties et consistant en la prestation de services de confiance. Ces données à caractère personnel seront conservées pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées, à condition que les signataires ne révoquent pas les consentements accordés. Par la suite, si nécessaire, les informations seront conservées de façon bloquée pendant les délais légalement établis, à l'issue desquels elles seront définitivement supprimées.

TROISIÈME. - DEVOIR DE CONFIDENTIALITÉ ET DE SECRET PROFESSIONNEL

### 3.1. Secret professionnel

Le SOUS-TRAITANT doit maintenir le secret professionnel à l'égard de toutes les données à caractère personnel du RESPONSABLE auxquelles il a accès à la suite de la fourniture des services établis dans le Contrat.

### 3.2. Obligation de confidentialité

Tout le personnel en charge du SOUS-TRAITANT qui accède et/ou traite des données personnelles est soumis au respect du secret professionnel et du devoir de confidentialité, obligations qui perdureront même après la fin de la fourniture des services.

En ce sens, seuls les employés du SOUS-TRAITANT qui ont besoin d'y accéder afin d'exercer leurs fonctions pour la fourniture de services peuvent accéder aux données personnelles.

Le SOUS-TRAITANT informera ses employés des obligations contenues dans le présent contrat et du caractère confidentiel des informations qu'ils traitent, tout en leur demandant de se conformer aux obligations qui peuvent leur être applicables conformément à la réglementation applicable, et les avertira de la responsabilité qu'ils encourraient s'ils les divulguaient.

En outre, tant dans le cas où les employés exécutent les services contractés dans les locaux du RESPONSABLE qu'à distance, le RESPONSABLE les informera opportunément des règles et procédures auxquelles ils sont soumis, ainsi que de toute autre disposition qu'ils doivent respecter conformément aux instructions fournies par le personnel du RESPONSABLE.

### 3.3. Violation de ces obligations et conséquences

La violation par le SOUS-TRAITANT ou le personnel à son service de l'obligation de confidentialité concernant les données susmentionnées ou de toute autre obligation découlant de la législation sur la protection des données à caractère personnel entraînera la résiliation du contrat principal et, par conséquent, du présent contrat.

## QUATRIÈME. - RESPECT DES INSTRUCTIONS PAR LE SOUS-TRAITANT

### 4.1. Obligation générale – Communications de données

Le SOUS-TRAITANT peut prendre toutes les décisions organisationnelles et opérationnelles nécessaires à la prestation du service pour lequel il a été engagé. Toutefois, les décisions qu'il prend doivent dans tous les cas respecter les instructions données par le RESPONSABLE.

Sans préjudice de ce qui précède, afin de respecter les dispositions relatives à la prestation du service, des communications de données peuvent avoir lieu entre les sociétés du groupe Signaturit à des fins administratives et d'assistance, ainsi que pour toutes celles nécessaires à la bonne prestation du service. Vous pouvez consulter la composition du Groupe Signaturit sur : <https://www.signaturit.com/fr/mentions-legales/>

### 4.2. Obligations spécifiques

Les obligations sont, entre autres, descriptives, mais sans s'y limiter, les suivantes :

#### 1. Obligations en matière de sécurité

Le FOURNISSEUR (ou, le cas échéant, le PRESTATAIRE final du service) dispose d'un système de **gestion de la sécurité de l'information (SGSI) mettant en œuvre les meilleures pratiques en matière de gestion de la sécurité de l'information** conformément à la norme UNE-ISO/IEC 27001, le Schéma national de sécurité et la norme ISO/IEC 22301, en appliquant à tous les traitements de données qu'il effectue dans le cadre des contrats conclus avec le CLIENT les contrôles et les mesures visant

à garantir la sécurité des données à caractère personnel relevant de la responsabilité du CLIENT auxquelles il a accès dans le cadre du contrat.

2. Ne pas appliquer ni utiliser les données à caractère personnel auxquelles il a accès dans l'exercice des fonctions qui lui ont été confiées à des fins autres que celles établies dans le présent contrat, et ne pas communiquer ces données, même à des fins de conservation, à des tiers, sauf si une loi ou une décision judiciaire en dispose autrement.
3. Le SOUS-TRAITANT est tenu de conserver sous son contrôle et sa garde les données personnelles fournies par le RESPONSABLE, et de ne pas les divulguer ni les transférer, même à des fins de conservation, à l'exception de ce qui est stipulé dans la clause six du présent contrat.
4. Dans tous les cas, l'accès et le traitement des données par le Titulaire seront soumis aux mesures de sécurité adoptées pour se conformer au principe de responsabilité proactive consacré à l'article 5.2 du RGPD.
5. Le personnel du Responsable du traitement doit s'engager expressément à respecter la confidentialité et à se conformer aux mesures de sécurité correspondant au traitement des données du RESPONSABLE.
6. Tenir, par écrit, un registre de toutes les catégories d'activités de traitement effectuées pour le compte du RESPONSABLE, contenant :
  - a. Le nom et les coordonnées du ou des sous-traitants et de chaque responsable pour le compte duquel le sous-traitant agit et, le cas échéant, du représentant du responsable ou du sous-traitant et du délégué à la protection des données.
  - b. Les catégories de traitements effectués par le sous-traitant.
  - c. Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l'identification dudit pays tiers ou de ladite organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, du RGPD, la documentation relative aux garanties appropriées.
  - d. Tenir un registre des mesures de sécurité applicables à ses systèmes, dans ce cas sur la base des normes de sécurité de l'information ISO / IEC 27001 et du Schéma national de sécurité.
7. Ne sous-traiter aucune des prestations faisant partie de l'objet du présent Contrat qui impliquent un traitement de données à caractère personnel découlant des dispositions du présent Contrat ou du contrat principal, à l'exception toutefois des services auxiliaires nécessaires au fonctionnement normal des services du SOUS-TRAITANT qui sont énumérés à l'annexe I.
  - a. Pour la sous-traitance de sous-traitants par le SOUS-TRAITANT, le RESPONSABLE doit en être informé par écrit au moins trente (30) jours à l'avance, en indiquant les traitements qui seront sous-traités et en identifiant clairement et sans ambiguïté la société sous-traitante et ses coordonnées. Le RESPONSABLE sera réputé avoir donné son consentement à la sous-traitance s'il ne fait pas part de son refus écrit au SOUS-TRAITANT dans un délai de trente (30) jours à compter de la notification.
  - b. Une fois la sous-traitance autorisée, le SOUS-TRAITANT signera un contrat de sous-traitance avec le sous-traitant, dont le contenu devra respecter la réglementation en vigueur en matière de protection des données et les obligations en matière de sécurité et de confidentialité figurant dans le présent contrat de sous-traitance.

- c. En cas de manquement de la part du SOUS-TRAITANT ULTERIOR, le SOUS-TRAITANT initial restera pleinement responsable envers le RESPONSABLE en ce qui concerne le respect des obligations.
- 8. Notifier sans délai au RESPONSABLE les violations de la sécurité affectant les données personnelles appartenant au RESPONSABLE dont il aurait eu connaissance dans tous les cas avant vingt-quatre (24) heures, par courrier électronique et de manière fiable.
  - a. La notification doit contenir toutes les informations jugées pertinentes pour la documentation et la communication de l'incident. Plus précisément, et dans la mesure où elles sont disponibles, les informations suivantes doivent être fournies:
    - i. Description de la nature de la violation de la sécurité des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés.
    - ii. Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations complémentaires peuvent être obtenues.
    - iii. Description des conséquences possibles de la violation de la sécurité des données à caractère personnel.
    - iv. Description des mesures prises ou proposées pour remédier à la violation de la sécurité des données à caractère personnel, y compris, le cas échéant, les mesures prises pour atténuer les effets négatifs potentiels.
  - b. Dans la mesure où il n'est pas possible de fournir les informations simultanément, celles-ci sont fournies progressivement et sans retard injustifié.
- 9. Aider le RESPONSABLE DU TRAITEMENT à :
  - a. Effectuer des analyses d'impact relatives à la protection des données, le cas échéant.
  - b. Consultations préalables avec l'autorité de contrôle, le cas échéant.
- 10. Fournir aux parties intéressées, en collaboration avec le RESPONSABLE, les informations nécessaires pour se conformer au devoir d'information des articles 13 et 14 du RGPD et de l'article 11 de la LOPDGDD. Le libellé et le format dans lesquels les informations seront fournies doivent être convenus avec le RESPONSABLE avant le début de la collecte des données.
- 11. Permettre au RESPONSABLE de réaliser des audits, sous forme d'entretiens ou de documents, à l'aide de questionnaires, afin de vérifier le bon respect des obligations incombant au SOUS-TRAITANT, conformément aux dispositions du présent Contrat. Dans tous les cas, les Parties déclarent que le RESPONSABLE :
  - a. il devra donner un préavis minimum de trente (30) jours au SOUS-TRAITANT et ne pourra dépasser un audit annuel, sauf si le SOUS-TRAITANT signale une faille de sécurité ayant un impact grave sur les données à caractère personnel ou s'il y a eu une sanction de la part d'une autorité de protection des données à l'encontre du SOUS-TRAITANT;
  - b. il prendra en charge l'intégralité du coût de l'audit (y compris tous les frais, dépenses et honoraires associés) et sa durée ne dépassera pas deux journées de travail complètes, quel que soit le format choisi par le RESPONSABLE, et n'exigera pas de la personne désignée un temps de travail supérieur aux deux journées susmentionnées. Si le temps et les ressources nécessaires sont estimés supérieurs à ceux indiqués, le FOURNISSEUR en informera

préalablement le CLIENT afin que celui-ci adapte la portée de l'audit pour la réduire à l'effort prévu ou accepte de prendre en charge les coûts du FOURNISSEUR. La fréquence de ces audits sera annuelle.

- c. ils ne doivent pas perturber l'activité habituelle du SOUS-TRAITANT. Dans tous les cas, les dates et les délais de réalisation de l'audit pourront être adaptés par le SOUS-TRAITANT en fonction de la disponibilité du personnel affecté à leur réalisation.
- d. dans le cas où il serait proposé de réaliser des audits documentaires consistant à remplir des documents ou des formulaires, le délai pour leur réalisation ne sera pas inférieur à trente (30) jours, ce délai pouvant être ajusté si le FOURNISSEUR le demande.

#### CINQUIÈME. - MESURES DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

Le SOUS-TRAITANT pourra avoir ou aura accès à des supports informatiques et documentaires appartenant au RESPONSABLE, tels que des données relatives aux clients potentiels ou finaux du CLIENT, ainsi qu'aux employés ou autres types d'utilisateurs (ci-après dénommés « Utilisateurs »). À ce titre, le SOUS-TRAITANT, en sa qualité de sous-traitant, s'engage à appliquer les mesures de sécurité suivantes:

1. Définition spécifique du traitement effectué. Le SOUS-TRAITANT fournit les services détaillés dans le contrat-cadre, pour lesquels il peut accéder aux données personnelles des personnes concernées dont le RESPONSABLE est le responsable, conformément à la réglementation en vigueur en matière de responsable du traitement ou de sous-traitant, selon le cas. Le tableau du point 2.2.1 Activités de traitement à réaliser dans le cadre des services souscrits indique l'activité de traitement du service souscrit.
2. Type d'accès. Le SOUS-TRAITANT a accès aux données informatiques ou documentaires du RESPONSABLE, le tout dans le but de fournir les services détaillés dans le contrat principal.
3. Lieu du traitement. Le traitement par le SOUS-TRAITANT s'effectuera sous forme documentaire ou informatisée, par l'envoi de rapports, de listes et d'informations sur les utilisateurs susmentionnés aux systèmes du RESPONSABLE, entre autres, lorsque cela est demandé.
4. Mesures de sécurité appliquées : Le SOUS-TRAITANT dispose des mesures de sécurité suivantes:
  - a. *Il dispose d'un système de désignation des noms d'utilisateur et des mots de passe de ses employés, tant pour ses propres systèmes que pour ceux de tiers, qui limite les accès en fonction des profils des utilisateurs, grâce à l'attribution de noms d'utilisateur personnalisés et de mots de passe qui expirent au moins une fois par an.*
  - b. *Il a informé son personnel des droits et devoirs qui lui incombent en matière de traitement des données de tiers, en indiquant expressément les données personnelles fournies par les clients.*
  - c. *Il dispose d'une liste actualisée des profils et des autorisations de ses utilisateurs, tant pour ses propres systèmes que pour ceux de tiers.*
  - d. *Il dispose d'un système d'enregistrement des incidents, ainsi que du protocole à suivre en cas d'incident interne ou vis-à-vis du RESPONSABLE, des utilisateurs ou de l'organisme de contrôle.*
  - e. *Il prendra les mesures appropriées pour le transfert des supports, propres ou tiers, le cas échéant.*
  - f. *Il dispose d'un inventaire actualisé des actifs.*
  - g. *Dispose d'un système de sauvegarde quotidienne de ses systèmes informatiques.*
  - h. *Un délégué à la protection des données a été désigné. Vous pouvez le contacter à l'adresse suivante : [dpo@signaturit.com](mailto:dpo@signaturit.com)*

- i. Elle a réalisé ou réalise tous les deux ans des audits en matière de protection des données.*
- j. Elle dispose d'un système d'enregistrement des entrées et sorties de supports pouvant contenir des données personnelles sensibles et qui respecte les paramètres de la loi.*
- k. Elle limite les accès non autorisés à ses systèmes informatiques, car elle dispose de zones sécurisées, avec un accès physique et logique limité.*
- l. Dans son circuit et son registre des incidents, il est également possible d'enregistrer le processus de récupération des données, conformément aux paramètres de la réglementation applicable.*
- m. Il applique dans leur intégralité les mesures de sécurité établies dans son système de gestion de la sécurité de l'information, qui est audité et certifié selon la norme ISO 27001.*

#### SIXIÈME. - ASSISTANCE DANS L'EXERCICE DES DROITS DES PARTIES INTÉRESSÉES

Le SOUS-TRAITANT doit assister le RESPONSABLE dans la réponse à l'exercice des droits suivants :

- Accès, rectification, suppression et opposition
- Limitation du traitement
- Portabilité des données
- Ne pas faire l'objet de décisions individualisées automatisées (y compris le profilage)

À cette fin, lorsque les personnes concernées exercent leurs droits d'accès, de rectification, de suppression et d'opposition, de limitation du traitement, de portabilité des données et de ne pas faire l'objet de décisions individuelles automatisées auprès du SOUS-TRAITANT du traitement, celui-ci doit en informer le Responsable par courrier électronique

La communication doit être effectuée immédiatement et en aucun cas au-delà du jour ouvrable suivant la réception de la demande, accompagnée, le cas échéant, d'autres informations pouvant être pertinentes pour répondre à la demande.

#### SEPTIÈME. - ENGAGEMENTS ET OBLIGATIONS DU RESPONSABLE

Le RESPONSABLE déclare respecter toutes les mesures techniques et organisationnelles nécessaires pour garantir la sécurité du traitement, des centres de traitement des données, des locaux, des équipements, des systèmes, des programmes et des personnes intervenant dans le traitement des données à caractère personnel susmentionnées, le tout étant reflété dans le document de sécurité auquel il est tenu conformément à la réglementation en vigueur.

Le RESPONSABLE est responsable des garanties des personnes concernées, telles que les droits d'accès, de rectification, d'annulation et d'opposition.

En utilisant les Services, le RESPONSABLE doit se conformer à la législation applicable. Par conséquent, toutes les instructions du RESPONSABLE relatives au traitement des données à caractère personnel doivent être conformes à la législation sur la protection des données et il est seul responsable de l'exactitude, de la qualité et de la légitimité de ces données à caractère personnel et des moyens par lesquels elles ont été obtenues.

Le RESPONSABLE s'engage à communiquer au SOUS-TRAITANT toute modification des données à caractère personnel fournies, afin que celui-ci procède à leur mise à jour.

#### HUITIÈME. - DURÉE ET RÉSILIATION DU CONTRAT

Le présent contrat est considéré comme accessoire à la prestation de services déterminée dans le contrat principal, de sorte que sa durée et son expiration sont soumises à ce lien ou contrat principal.

À l'expiration du contrat, le SOUS-TRAITANT devra restituer au responsable du traitement les données à caractère personnel et, le cas échéant, les supports sur lesquels elles sont enregistrées, une fois la prestation effectuée, sauf dans les cas où leur destruction est appropriée ou possible, auquel cas celle-ci sera effectuée après en avoir informé le RESPONSABLE et après certification a posteriori que celle-ci a bien été effectuée.

Dans tous les cas, la restitution doit entraîner la suppression totale des données existantes sur les équipements informatiques utilisés par le sous-traitant. Toutefois, le SOUS-TRAITANT peut conserver une copie, avec les données dûment bloquées, tant que des responsabilités peuvent découler de l'exécution de la prestation, afin de respecter les engagements légaux du SOUS-TRAITANT, en respectant toujours les principes de confidentialité et de minimisation des données.

#### NEUVIÈME. LOI APPLICABLE ET JURIDICTION

Le présent contrat sera régi par les clauses qu'il contient et, en l'absence de dispositions contraires, par la réglementation espagnole et européenne applicable en matière de traitement des données à caractère personnel.

Pour soumettre les litiges relatifs à l'interprétation ou à l'application du présent contrat, toute question sera régie par les dispositions convenues par les parties dans le contrat de prestation de services ou les conditions générales de vente.