

# Contrat de sous-traitance

Traitement des données à caractère personnel pour le compte du Praticien — article 28 du RGPD

Version 1.7

Septembre 2026

Praticien (responsable de traitement) ↔ Bloom Lab (sous-traitant)

## Entre les soussignés

**Le Praticien**, exerçant la profession de psychologue / psychothérapeute en qualité de professionnel libéral, **identifié par le Compte au titre duquel le présent contrat est accepté** — nom, prénom, numéro RPPS ou ADELI le cas échéant, adresse professionnelle et adresse électronique tels que renseignés dans son Compte,

ci-après désigné « **le Praticien** » ou « **le Responsable de traitement** »,

d'une part,

Et

**Bloom Lab, SARL** au capital de **30 000** euros, immatriculée au registre du commerce et des sociétés de **Paris** sous le numéro **989 596 408**, dont le siège social est situé 58 rue de Monceau, CS 48756, 75008 Paris, représentée par **Mickaël Quemerais Lefel**, en qualité de **gérant**, éditeur de l'application **Annota**,

ci-après désignée « **l'Éditeur** » ou « **le Sous-traitant** »,

d'autre part,

Ci-après désignés ensemble « les Parties » et individuellement « une Partie ».

## Il a été préalablement exposé ce qui suit

Le Praticien exerce une activité de suivi psychologique. À ce titre, il tient des dossiers relatifs à ses patients, comportant des données concernant la santé au sens de l'article 9 du règlement (UE) 2016/679 (ci-après le « RGPD »), couvertes par le secret professionnel.

L'Éditeur met à disposition du Praticien l'application Annota, un service de tenue du dossier patient permettant notamment la rédaction de comptes rendus de séance par dictée, la numérisation et l'indexation de documents, ainsi que la recherche au sein d'un dossier, avec l'assistance de traitements automatisés recourant à l'intelligence artificielle.

L'exécution de ce service conduit l'Éditeur à traiter, pour le compte et sur instruction du Praticien, des données à caractère personnel relevant de la responsabilité de ce dernier. Les Parties entendent définir, par le présent contrat, les conditions de ce traitement conformément à l'article 28 du RGPD.

Le présent contrat s'inspire des clauses contractuelles types entre responsables du traitement et sous-traitants adoptées par la Commission européenne dans sa décision d'exécution (UE) 2021/915 du 4 juin 2021, adaptées au service Annota.

Ceci exposé, il a été convenu ce qui suit.

## Article 1 — Définitions

Les termes ci-après ont, dans le présent contrat, le sens suivant :

- **RGPD** : le règlement (UE) 2016/679 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.
- **Loi Informatique et Libertés** : la loi n° 78-17 du 6 janvier 1978 modifiée.
- **Données** : les données à caractère personnel traitées par l'Éditeur pour le compte du Praticien dans le cadre du Service, telles que décrites à l'Annexe 1.
- **Données de santé** : les données concernant la santé au sens de l'article 4.15 du RGPD, relevant de la catégorie particulière visée à l'article 9.1 du même règlement.
- **Personne concernée** : la personne physique à laquelle se rapportent les Données, principalement le patient du Praticien.
- **Service** : l'application Annota et les services associés fournis par l'Éditeur, accessibles par deux canaux — l'**application mobile** (iOS, Android) installée sur le terminal du Praticien et la **version bureau** exécutée dans le navigateur d'un ordinateur, sans installation — ainsi que l'interface de programmation, l'hébergement et les traitements automatisés qui les servent. Le canal d'accès est sans incidence sur la localisation et le régime des Données, qui demeurent hébergées et traitées dans les conditions de l'article 9.
- **Sous-traitant ultérieur** : toute personne à laquelle l'Éditeur confie tout ou partie de l'exécution des traitements réalisés pour le compte du Praticien.
- **Violation de données** : une violation de la sécurité au sens de l'article 4.12 du RGPD.
- **HDS** : l'hébergement de données de santé à caractère personnel soumis à certification en application de l'article L. 1111-8 du code de la santé publique.

## Article 2 — Objet et documents contractuels

---

2.1. Le présent contrat a pour objet de définir les conditions dans lesquelles l'Éditeur, agissant en qualité de sous-traitant, traite pour le compte du Praticien les Données nécessaires à la fourniture du Service, ainsi que les obligations respectives des Parties au titre du RGPD.

2.2. Le présent contrat constitue une annexe indissociable des conditions générales d'utilisation et de vente du Service. Il s'applique pendant toute la durée d'utilisation du Service, y compris pendant une éventuelle phase d'essai ou de version bêta.

2.3. En cas de contradiction entre le présent contrat et tout autre document contractuel liant les Parties, les stipulations du présent contrat prévalent pour tout ce qui concerne la protection des données à caractère personnel.

## Article 3 — Rôle des parties

---

3.1. Le Praticien est **responsable de traitement** des Données figurant dans les dossiers patients qu'il tient au moyen du Service. Il détermine seul les finalités et les moyens essentiels de ce traitement, la licéité de sa collecte, le contenu des dossiers, la durée de conservation applicable et les destinataires éventuels.

3.2. L'Éditeur est **sous-traitant** de ce traitement. Il n'agit que sur instruction documentée du Praticien, dans les conditions définies à l'article 6.

3.3. L'Éditeur est en revanche **responsable de traitement** pour ses propres traitements, distincts du dossier patient, notamment : la gestion du compte du Praticien et de son authentification, la facturation de l'abonnement, l'assistance aux utilisateurs, la sécurité du Service et les statistiques d'usage anonymes. Ces traitements sont décrits dans la politique de confidentialité du Service. Ils ne portent sur aucun contenu clinique des dossiers patients ; les journaux techniques produits au titre de la sécurité peuvent toutefois comporter des identifiants techniques (identifiants de compte, de dossier ou de requête), à l'exclusion de tout contenu, et sont traités avec le même niveau de protection que les Données.

3.4. Lorsque plusieurs praticiens exercent au sein d’une même structure, chacun demeure responsable de traitement pour les dossiers qu’il tient, sauf convention contraire écrite entre eux et portée à la connaissance de l’Éditeur.

## Article 4 — Description des traitements

---

4.1. La nature, la finalité, la durée des traitements, les catégories de Données et de personnes concernées sont décrites à l’**Annexe 1**, qui fait partie intégrante du présent contrat.

4.2. Le Praticien peut compléter cette description par des instructions écrites, dans les limites des fonctionnalités du Service. Toute instruction excédant ces fonctionnalités fait l’objet d’un accord préalable entre les Parties et, le cas échéant, d’un devis.

## Article 5 — Durée

---

5.1. Le présent contrat entre en vigueur à la date de sa signature ou, à défaut, à la date d’acceptation des conditions générales du Service par le Praticien, et demeure en vigueur pendant toute la durée de fourniture du Service.

5.2. Les obligations relatives à la confidentialité, à la sécurité, à la notification des violations et au sort des Données en fin de contrat survivent à son terme jusqu’à leur complète exécution.

## Article 6 — Obligations générales du Sous-traitant

---

6.1. **Traitement sur instruction documentée.** L’Éditeur ne traite les Données que sur instruction documentée du Praticien. Constituent des instructions documentées : le présent contrat et ses annexes, les conditions générales du Service, les paramétrages et les actions effectués par le Praticien au moyen du Service, ainsi que toute demande écrite adressée par le Praticien à l’Éditeur.

6.2. **Instruction illicite.** L’Éditeur informe immédiatement le Praticien s’il estime qu’une instruction constitue une violation du RGPD, de la loi Informatique et Libertés ou de toute autre disposition du droit de l’Union ou du droit français relative à la protection des données. L’Éditeur peut suspendre l’exécution de l’instruction concernée jusqu’à sa confirmation ou sa modification par le Praticien.

6.3. **Obligation légale de traiter.** Si le droit de l’Union ou le droit français impose à l’Éditeur de traiter les Données au-delà des instructions du Praticien, l’Éditeur en informe le Praticien avant le traitement, sauf si ce droit l’interdit pour des motifs importants d’intérêt public.

6.4. **Absence d’usage propre.** L’Éditeur s’interdit d’utiliser les Données à ses propres fins. Il s’interdit notamment, sans que cette liste soit limitative, de les céder, louer ou communiquer à des tiers, de les exploiter à des fins commerciales, publicitaires ou de prospection, de les utiliser à des fins de recherche, ainsi que de les utiliser, directement ou par l’intermédiaire d’un sous-traitant ultérieur, pour entraîner, affiner ou évaluer un modèle d’intelligence artificielle.

6.5. **Statistiques anonymes.** L’Éditeur peut produire des statistiques d’usage agrégées et anonymes (par exemple le nombre de comptes rendus créés ou la durée moyenne d’un traitement) aux fins d’amélioration et de dimensionnement du Service. Ces statistiques ne comportent aucun contenu de dossier patient et résultent d’un procédé d’**anonymisation irréversible** : elles ne permettent, ni directement ni indirectement, y compris par recoupement, la réidentification d’une personne concernée. Des données simplement pseudonymisées ne sont pas réputées anonymes au sens du présent article ; à défaut de pouvoir garantir l’anonymisation, la statistique n’est pas produite.

6.6. **Protection des données dès la conception.** L’Éditeur met en œuvre les principes de protection des données dès la conception et par défaut (article 25 du RGPD), notamment par la minimisation des données collectées, la suppression automatique des enregistrements audio après transcription et l’absence de captation de la voix du patient.

## Article 7 — Confidentialité et secret professionnel

---

7.1. L'Éditeur veille à ce que les personnes autorisées à traiter les Données s'engagent à en respecter la confidentialité par un engagement écrit, ou soient soumises à une obligation légale appropriée de confidentialité. Cet engagement survit à la cessation de leurs fonctions.

7.2. L'Éditeur reconnaît que les Données sont couvertes par le secret professionnel auquel le Praticien est tenu, notamment au titre de l'article 226-13 du code pénal, et qu'il est tenu à la même discrétion en sa qualité de prestataire intervenant sur des données de santé.

7.3. **Principe de non-accès.** L'architecture du Service est conçue pour que l'Éditeur n'accède pas au contenu des dossiers patients. L'accès à l'**environnement de production** (infrastructure, base de données, journaux techniques) est limité aux personnes strictement nécessaires à l'administration technique et à la sécurité du Service, sur la base du besoin d'en connaître ; il ne comporte pas, en fonctionnement normal, de consultation du contenu des dossiers. Tout accès au **contenu** d'un dossier est régi exclusivement par l'article 7.4.

7.4. L'Éditeur n'accède au contenu d'un dossier que dans deux cas : (a) à la demande écrite et circonstanciée du Praticien, pour les seuls besoins de la résolution d'un incident ; (b) lorsqu'une intervention est strictement nécessaire, en urgence, à la sécurité ou à l'intégrité du Service — le Praticien en étant alors informé sans délai. Dans les deux cas, l'accès est limité à ce qui est nécessaire, tracé, et le Praticien est informé de la clôture de l'intervention.

7.5. L'Éditeur sensibilise et forme les personnes intervenant sur le Service aux exigences applicables aux données de santé.

## Article 8 — Sécurité des traitements

---

8.1. L'Éditeur met en œuvre les mesures techniques et organisationnelles appropriées prévues à l'article 32 du RGPD, décrites à l'**Annexe 3**, afin de garantir un niveau de sécurité adapté au risque, en tenant compte du caractère sensible des Données.

8.2. L'Éditeur peut faire évoluer ces mesures pour tenir compte de l'état de l'art et de l'évolution des menaces, sans que le niveau de sécurité global puisse être diminué. Toute modification substantielle est portée à la connaissance du Praticien.

8.3. L'Éditeur procède à une revue périodique de ses mesures de sécurité. Il fait réaliser un test d'intrusion par un prestataire indépendant **dans les douze (12) mois suivant l'ouverture du Service au traitement de données réelles, puis au moins une fois par an**. Dans l'attente du premier test, l'Éditeur s'appuie sur une **revue de sécurité interne documentée**, conduite selon des référentiels reconnus (notamment ceux de l'OWASP) et dont les constats sont corrigés sans délai. Une synthèse de la dernière revue ou du dernier test est communiquée au Praticien sur demande.

## Article 9 — Localisation des données et hébergement de données de santé

---

9.1. **Hébergement certifié HDS.** Les Données sont hébergées auprès d'un hébergeur certifié pour l'hébergement de données de santé à caractère personnel conformément à l'article L. 1111-8 du code de la santé publique. L'hébergeur retenu, sa certification et son périmètre figurent à l'**Annexe 2**. Une copie du certificat est communiquée au Praticien sur demande.

9.2. **Localisation.** Les Données sont hébergées et traitées exclusivement sur le territoire de l'Union européenne, en France pour l'hébergement principal. L'Éditeur ne procède à aucun transfert de Données vers un pays tiers ni à aucune communication à une organisation internationale.

9.3. **Accès distant.** L'Éditeur garantit qu'aucun accès aux Données, y compris à des fins d'administration ou de maintenance, n'est réalisé depuis un pays situé hors de l'Espace économique européen.

9.4. **Réglementations extra-européennes.** L'Éditeur informe le Praticien, à sa connaissance et sur la base des informations communiquées par ses sous-traitants ultérieurs, de toute réglementation extra-européenne susceptible de permettre un accès aux Données par une autorité d'un pays tiers. À la date des présentes, l'Éditeur n'a connaissance d'aucune réglementation de cette nature applicable aux sous-traitants ultérieurs listés à l'Annexe 2, tous établis dans l'Union européenne.

9.5. Si une modification de l'architecture du Service devait entraîner un traitement hors de l'Union européenne, l'Éditeur en informerait le Praticien préalablement, dans les conditions de l'article 10.3, et mettrait en place les garanties appropriées prévues au chapitre V du RGPD.

## Article 10 — Sous-traitants ultérieurs

---

10.1. **Autorisation générale.** Le Praticien autorise l'Éditeur à recourir aux sous-traitants ultérieurs listés à l'Annexe 2 pour l'exécution du Service. Cette autorisation est donnée sur le fondement de l'article 28.2 du RGPD (autorisation écrite générale).

10.2. **Obligations répercutées.** L'Éditeur impose contractuellement à chaque sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles prévues au présent contrat, notamment quant à la sécurité, à la localisation des données dans l'Union européenne, à l'absence d'usage propre et à l'absence d'entraînement de modèles. L'Éditeur demeure pleinement responsable envers le Praticien de l'exécution de leurs obligations.

10.3. **Information préalable.** L'Éditeur informe le Praticien de tout projet d'ajout ou de remplacement d'un sous-traitant ultérieur au moins **trente (30) jours** avant sa mise en œuvre, par message électronique à l'adresse associée au compte et par une mention dans le Service.

10.4. **Droit d'opposition.** Le Praticien peut s'opposer à ce changement, par écrit et pour un motif tenant à la protection des données, dans un délai de **quinze (15) jours** suivant l'information. À défaut d'accord entre les Parties, le Praticien peut résilier le Service sans frais ni pénalité, avec restitution de ses données dans les conditions de l'article 15, l'abonnement étant remboursé au prorata de la période non consommée.

10.5. L'Éditeur communique au Praticien, sur demande, une copie des engagements de protection des données souscrits par ses sous-traitants ultérieurs, le cas échéant expurgée des informations commerciales confidentielles.

## Article 11 — Traitements assistés par intelligence artificielle

---

11.1. **Finalités limitées.** Les traitements automatisés recourant à l'intelligence artificielle sont mis en œuvre aux seules fins de mise en forme et d'exploitation documentaire du dossier, à savoir : la transcription de la dictée du Praticien, la structuration du compte rendu selon une trame choisie par lui, la lecture automatique des documents numérisés (reconnaissance de caractères), l'indexation et la recherche au sein d'un dossier, ainsi que la production de résumés.

11.2. **Absence de finalité diagnostique.** Le Service ne produit aucun diagnostic, aucune évaluation clinique automatisée ni aucune recommandation thérapeutique. Il ne constitue pas un dispositif médical. Aucune décision produisant des effets juridiques ou affectant significativement une personne n'est prise sur le fondement d'un traitement exclusivement automatisé.

11.3. **Validation humaine.** Tout contenu produit par un traitement automatisé est identifié comme tel et n'est intégré au dossier qu'après validation expresse du Praticien, qui en demeure l'auteur au plan clinique et déontologique. Cette validation ne décharge pas l'Éditeur de sa responsabilité au titre d'un défaut du Service, d'une mauvaise exécution de ses obligations ou d'une violation du présent contrat.

11.4. **Absence d'entraînement et de conservation.** Le fournisseur de modèles auquel l'Éditeur recourt, identifié à l'Annexe 2, est contractuellement tenu de ne conserver aucun contenu transmis au-delà du temps strictement nécessaire à la production de la réponse (mode dit « Zero Data Retention », activé au niveau de l'organisation de l'Éditeur) et de ne

l'utiliser pour l'entraînement d'aucun modèle. Ce mode couvre l'ensemble des interfaces de programmation utilisées par le Service, toutes sans état : la transcription vocale, la génération de texte (structuration des comptes rendus, résumés, recherche documentaire) et la reconnaissance optique de caractères. Aucune autre fonction du fournisseur n'est utilisée. L'attestation d'activation et l'accord de sous-traitance du fournisseur sont conservés au dossier de conformité de l'Éditeur et communiqués au Praticien sur demande.

**11.5. Minimisation.** L'enregistrement audio de la dictée est supprimé dès la transcription effectuée, y compris en cas d'échec du traitement. La voix du patient n'est jamais captée : seule la dictée du Praticien, postérieure à la séance, est enregistrée. Le texte des questions posées à la fonction de recherche n'est pas conservé.

**11.6. Transparence à l'égard des patients (RGPD).** L'Éditeur communique au Praticien les informations nécessaires pour que celui-ci puisse informer ses patients du recours à des traitements assistés par intelligence artificielle, au titre des articles 13 et 14 du RGPD, notamment au moyen du modèle de note d'information mis à disposition dans le Service.

**11.7. Règlement (UE) 2024/1689 sur l'intelligence artificielle.** L'utilisateur direct des fonctions d'intelligence artificielle du Service est le Praticien, professionnel informé de leur nature par le présent contrat et par le Service lui-même, qui identifie les contenus générés. L'Éditeur documente, fonction par fonction, la qualification du Service au regard de ce règlement (rôle de fournisseur ou de déployeur, catégorie de système, obligations de transparence de l'article 50 applicables) et tient cette analyse à la disposition du Praticien. Il l'informe de toute évolution de cette qualification emportant des obligations nouvelles pour le Praticien.

## Article 12 — Assistance au Responsable de traitement

---

**12.1. Droits des personnes concernées.** L'Éditeur met à la disposition du Praticien, au sein du Service, les fonctionnalités permettant de répondre aux demandes d'exercice des droits : consultation et rectification des données d'un dossier, export complet d'un dossier dans un format lisible, suppression d'un dossier, consultation du journal des accès.

**12.2.** Compte tenu de ces fonctionnalités, le Praticien traite lui-même les demandes des personnes concernées. Lorsqu'une demande excède les possibilités offertes par le Service, l'Éditeur apporte au Praticien une assistance raisonnable, dans un délai lui permettant de respecter les délais légaux de réponse.

**12.3. Demandes reçues directement.** Si une personne concernée s'adresse directement à l'Éditeur, celui-ci s'abstient d'y répondre au fond, informe la personne qu'elle doit s'adresser au Praticien et transmet la demande au Praticien dans un délai maximum de **cinq (5) jours ouvrés**.

**12.4. Autres obligations.** L'Éditeur assiste le Praticien, dans la limite des informations dont il dispose, pour le respect des obligations prévues aux articles 32 à 36 du RGPD, notamment la sécurité des traitements, la notification des violations, l'analyse d'impact relative à la protection des données et la consultation préalable de l'autorité de contrôle.

**12.5.** L'Éditeur met à la disposition du Praticien les éléments documentaires utiles à ces obligations : description des mesures de sécurité, liste des sous-traitants ultérieurs, éléments relatifs à l'hébergement certifié HDS et, le cas échéant, l'analyse d'impact réalisée par l'Éditeur au titre du Service.

**12.6. Autorités de contrôle.** L'Éditeur informe le Praticien de toute demande émanant d'une autorité de contrôle ou d'une autorité judiciaire portant sur les Données, sauf interdiction légale, et ne communique aucune Donnée sans en avoir préalablement informé le Praticien, sauf lorsque la loi l'impose.

## Article 13 — Violation de données à caractère personnel

---

**13.1.** L'Éditeur alerte le Praticien de toute violation de données affectant les Données **sans délai injustifié et au plus tard vingt-quatre (24) heures** après en avoir pris connaissance, **même lorsque les informations disponibles sont encore incomplètes**, par message électronique adressé à l'adresse associée au compte du Praticien, doublé d'un appel

téléphonique en cas de violation présentant un risque élevé. Le délai court à compter de la connaissance de la violation par l'Éditeur ; l'hébergeur s'engage de son côté à notifier l'Éditeur de tout incident dans un délai maximum de soixante-douze (72) heures (contrat d'hébergement de données de santé du 26 août 2026, article 6).

13.2. La notification comporte les éléments listés à l'**Annexe 4**, dans la mesure où ils sont disponibles. Les informations manquantes sont communiquées de manière échelonnée, sans retard indu, et un point de situation est adressé au Praticien **au moins tous les trois (3) jours** jusqu'à la clôture de l'incident.

13.3. L'Éditeur documente toute violation, ses effets et les mesures correctrices prises, et tient cette documentation à la disposition du Praticien et de l'autorité de contrôle.

13.4. La notification à l'autorité de contrôle prévue à l'article 33 du RGPD et, le cas échéant, la communication aux personnes concernées prévue à l'article 34, incombent au Praticien en sa qualité de responsable de traitement. L'Éditeur lui apporte l'assistance nécessaire et ne procède à aucune notification en son nom, sauf mandat écrit exprès.

13.5. L'Éditeur prend sans délai toute mesure utile pour mettre fin à la violation, en limiter les effets et empêcher son renouvellement.

## Article 14 — Durées de conservation

---

14.1. Le Praticien détermine, sous sa responsabilité, les durées de conservation applicables aux dossiers qu'il tient. **Le Service ne propose aucune durée par défaut** : le Praticien définit explicitement la durée applicable, pour l'ensemble de ses dossiers ou dossier par dossier. Pour l'éclairer, l'Éditeur met à sa disposition une **documentation de conservation** exposant les références applicables (notamment le référentiel de la Commission nationale de l'informatique et des libertés relatif aux cabinets médicaux et paramédicaux et les recommandations propres à chaque profession), en distinguant conservation en base active, archivage intermédiaire et suppression. Cette documentation est indicative et ne dispense pas le Praticien d'apprécier ses propres obligations légales et déontologiques.

14.2. Aucune suppression n'est opérée automatiquement par le Service : à l'échéance de la durée définie par le Praticien, le Service lui signale les dossiers concernés et lui propose de procéder à leur suppression, qui demeure une décision du Praticien.

14.3. Durées particulières appliquées par l'Éditeur :

- enregistrement audio de la dictée : supprimé dès la transcription, sans conservation ;
- copie locale du dossier sur le terminal du Praticien (**application mobile uniquement**) : conservée au maximum **sept (7) jours** et purgée à la déconnexion ; **la version bureau ne conserve aucune copie locale du dossier** — les Données affichées ne subsistent que dans la mémoire de l'onglet et disparaissent à sa fermeture (annexe 3, § 0 et § 3) ;
- journal des accès : conservé **douze (12) mois**, durée justifiée par les besoins de traçabilité des accès à des données de santé ;
- données de compte du Praticien : conservées pendant la durée de l'abonnement, puis supprimées dans les conditions de l'article 15 ;
- données de facturation traitées par l'Éditeur en qualité de responsable de traitement : dix (10) ans, en application des obligations comptables.

## Article 15 — Réversibilité et sort des données en fin de contrat

---

15.1. **Pendant le contrat.** Le Praticien peut, à tout moment et sans frais, exporter les dossiers qu'il tient au moyen du Service : dans un **format lisible** (document mis en page et texte brut) et dans un **format structuré, couramment utilisé et lisible par machine (JSON)** comportant l'intégralité du dossier — contenus, pièces versées dans leur format

d'origine, métadonnées (dates, statuts, liens entre documents) et journal des accès — de manière à permettre une réutilisation effective dans un autre outil.

15.2. **À la fin du contrat.** Le Praticien dispose d'un délai de **trente (30) jours** à compter de la cessation du Service pour procéder à l'export de ses données. L'Éditeur maintient l'accès nécessaire à cet export pendant ce délai.

15.3. À l'expiration de ce délai, et sauf instruction contraire écrite du Praticien, l'Éditeur procède à la suppression définitive de l'ensemble des Données de l'environnement de production dans un délai de **trente (30) jours**. Les Données subsistant dans les sauvegardes sont supprimées à l'issue du cycle de rotation de celles-ci, qui n'excède pas **trente-cinq (35) jours** supplémentaires ; jusqu'à leur purge, ces sauvegardes résiduelles demeurent chiffrées, isolées et inaccessibles en exploitation courante, et ne font l'objet d'aucune restauration sauf obligation légale.

15.4. L'Éditeur ne conserve, au-delà de ces délais, que les données dont la conservation est imposée par une obligation légale, pour la seule durée de cette obligation et à cette seule fin.

15.5. Une attestation de suppression est délivrée au Praticien sur simple demande.

15.6. Le Praticien demeure responsable de la conservation du dossier de ses patients conformément à ses obligations déontologiques et légales ; il lui appartient, avant toute suppression, de s'assurer qu'il en conserve une copie ou qu'il en a organisé la reprise.

## Article 16 — Documentation, audits et vérifications

---

16.1. L'Éditeur met à la disposition du Praticien toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD, notamment : le présent contrat et ses annexes, le certificat HDS de l'hébergeur, la liste et les engagements des sous-traitants ultérieurs, la description des mesures de sécurité et la synthèse de la dernière revue de sécurité ou du dernier test d'intrusion.

16.2. Le Praticien peut faire réaliser un audit de conformité **une (1) fois par année civile**, sous réserve d'un préavis écrit de **trente (30) jours**, pendant les heures ouvrées, et sans perturber l'exploitation du Service. Par exception, un audit peut être diligenté **sans limitation de fréquence et avec un préavis ramené à quarante-huit (48) heures** : à la suite d'une violation de données significative, sur demande d'une autorité de contrôle, ou en cas d'urgence ou de suspicion raisonnable et documentée d'un manquement de l'Éditeur à ses obligations.

16.3. L'auditeur éventuellement mandaté ne doit pas être un concurrent de l'Éditeur et est tenu à une obligation de confidentialité. L'audit ne peut porter atteinte à la sécurité ni à la confidentialité des données des autres clients de l'Éditeur ; il ne comporte aucun accès aux données de production d'autres praticiens.

16.4. Les frais d'audit sont à la charge du Praticien, sauf si l'audit révèle un manquement substantiel de l'Éditeur à ses obligations, auquel cas ils sont supportés par l'Éditeur, qui met en œuvre à ses frais un plan de correction dans un délai raisonnable.

16.5. L'Éditeur peut satisfaire à une demande d'audit en communiquant les résultats d'un audit mutualisé, réalisé par un tiers indépendant et portant sur le même périmètre, dès lors que ces résultats sont suffisamment récents et complets.

## Article 17 — Registre des catégories d'activités de traitement

---

L'Éditeur tient un registre des catégories d'activités de traitement effectuées pour le compte du Praticien, conformément à l'article 30.2 du RGPD. Il le communique à l'autorité de contrôle sur demande et en informe le Praticien.

## Article 18 — Point de contact

---

18.1. Le point de contact de l'Éditeur pour toute question relative au présent contrat est : **contact@annota.fr** — Bloom Lab, 58 rue de Monceau, CS 48756, 75008 Paris. Les questions relatives à la protection des données peuvent être

adressées à l'adresse dédiée : [rgpd@annota.fr](mailto:rgpd@annota.fr).

18.2. L'Éditeur n'a pas désigné de délégué à la protection des données à la date des présentes ; l'analyse de cette obligation (article 37.1 du RGPD) est documentée et réexaminée à mesure de la croissance du Service. En cas de désignation, l'identité et les coordonnées du délégué sont communiquées au Praticien et publiées dans la politique de confidentialité.

18.3. Le point de contact du Praticien est **l'adresse électronique associée à son Compte**, telle que renseignée par lui. Le Praticien informe l'Éditeur de tout changement de cette adresse, notamment parce qu'elle est utilisée pour la notification des violations de données.

## Article 19 — Responsabilité et assurance

19.1. Chaque Partie répond des dommages qu'elle cause du fait d'un traitement non conforme, dans les conditions de l'article 82 du RGPD.

19.2. L'Éditeur déclare avoir souscrit une assurance de responsabilité civile professionnelle couvrant les conséquences pécuniaires de sa responsabilité, auprès de **Hiscox SA** (agissant par sa succursale française), **police n° HSXIN320088911A** (« Métiers de l'Informatique et du Digital »), à hauteur de **50 000 € par sinistre et par année d'assurance** en responsabilité civile professionnelle. Cette police comporte en outre un volet **cyber** (garantie « Toutes garanties cyber », 50 000 € par sinistre et par année) couvrant notamment l'assistance en cas de cyberattaque, la prise en charge des enquêtes et sanctions administratives (y compris les amendes prononcées par l'autorité de contrôle), la reconstitution des données de l'Éditeur, les dommages causés aux tiers et la cyber-extorsion. Une attestation d'assurance est communiquée au Praticien sur demande.

19.3. **Limitation de responsabilité.** Sous réserve des dispositions impératives applicables, la responsabilité totale cumulée de l'Éditeur à l'égard du Praticien au titre du présent contrat est plafonnée au **montant le plus élevé entre (i) les redevances effectivement versées par le Praticien au cours des douze (12) mois précédant le fait générateur du dommage et (ii) un montant forfaitaire de vingt-cinq mille (25 000) euros**. Lorsque le Service est fourni à titre gratuit ou depuis moins de douze mois, le montant visé au (i) est réputé égal à douze (12) mensualités du tarif public en vigueur. Ce plafond ne s'applique pas : (a) en cas de dol, de fraude, de faute lourde ou de manquement délibéré de l'Éditeur ; (b) aux atteintes à la confidentialité des Données et au secret professionnel ; (c) aux dommages corporels. Il ne limite en rien le droit à réparation des personnes concernées prévu à l'article 82 du RGPD, ni la répartition des responsabilités entre responsable de traitement et sous-traitant organisée par ce même article. Cette clause est alignée sur la clause correspondante des conditions générales de vente (article 13.2), le présent contrat prévalant en matière de protection des données (article 2.3).

## Article 20 — Modification du contrat

20.1. Le présent contrat peut être modifié pour tenir compte de l'évolution de la réglementation, des recommandations de l'autorité de contrôle ou de l'architecture du Service.

20.2. Les modifications **strictement commandées par une évolution de la réglementation ou par une recommandation d'une autorité de contrôle** sont portées à la connaissance du Praticien et s'appliquent à la date requise par cette évolution, sans pouvoir réduire le niveau de protection des Données. **Toute autre modification substantielle** est portée à la connaissance du Praticien au moins **trente (30) jours** avant son entrée en vigueur et requiert son acceptation ; à défaut d'acceptation, le Praticien peut résilier le Service sans frais, avec restitution de ses données dans les conditions de l'article 15.

20.3. La mise à jour de l'Annexe 2 (sous-traitants ultérieurs) obéit à la procédure spécifique de l'article 10. La mise à jour de l'Annexe 3 (mesures de sécurité) obéit à l'article 8.2 : les évolutions qui ne diminuent pas le niveau de sécurité

global sont portées à la connaissance du Praticien et s'appliquent dès leur publication, sans préavis ni acceptation préalable.

## Article 21 — Droit applicable et différends

---

21.1. Le présent contrat est soumis au droit français.

21.2. Les Parties s'efforcent de résoudre à l'amiable tout différend relatif à son interprétation ou à son exécution. À défaut d'accord dans un délai de trente (30) jours, **tout différend relève des juridictions territorialement compétentes selon les règles de droit commun.**

21.3. Le présent article ne fait pas obstacle au droit de toute personne concernée d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés ou d'exercer un recours juridictionnel.

## Acceptation du contrat

---

Le présent contrat est accepté par le Praticien **par voie électronique**, lors de la création de son Compte ou lors d'une réacceptation, par une action positive consistant à cocher la case prévue à cet effet. Ce mode d'acceptation est admis par l'article 28.9 du RGPD et par l'article 4.1 des conditions générales d'utilisation et de vente.

**La date et l'heure de l'acceptation, l'identifiant du Compte et la version acceptée du présent contrat sont conservés par l'Éditeur à des fins probatoires.** Aucune signature manuscrite n'est requise.

L'Éditeur, Bloom Lab, est partie au contrat en sa qualité d'éditeur du Service ; il met le présent contrat à disposition, dans sa version en vigueur, sur annota.fr et dans l'espace « Conformité » du Compte du Praticien.

## Annexe 1 — Description détaillée des traitements

| Rubrique                                          | Description                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nature du traitement                              | Collecte, enregistrement, organisation, structuration, conservation, adaptation, extraction, consultation, transcription automatique de la parole, reconnaissance optique de caractères, indexation sémantique, recherche, production de résumés, export et effacement.                                                        |
| Finalités                                         | Fournir au Praticien un service de tenue et de consultation du dossier patient : rédaction assistée des comptes rendus de séance à partir de sa dictée, classement et lecture des documents numérisés, recherche et résumé au sein d'un dossier, export et suppression du dossier.                                             |
| Canaux d'accès                                    | Application mobile (iOS, Android) installée sur le terminal du Praticien ; version bureau exécutée dans le navigateur d'un ordinateur, sans installation. Le canal est sans incidence sur la localisation et le régime des Données (article 9) ; il détermine en revanche certaines mesures de sécurité décrites à l'annexe 3. |
| Catégories de personnes concernées                | Les patients du Praticien, y compris des mineurs ; les tiers éventuellement mentionnés dans les comptes rendus ou les documents versés au dossier (membres de l'entourage, autres professionnels de santé) ; le Praticien lui-même au titre de son compte utilisateur.                                                         |
| Catégories de données — identification            | Nom, prénom, date de naissance, adresse électronique, numéro de téléphone du patient.                                                                                                                                                                                                                                          |
| Catégories de données — santé (article 9 du RGPD) | Motif de consultation, anamnèse, comptes rendus de séance, observations cliniques, documents numérisés versés au dossier (courriers d'adressage, ordonnances, bilans) et leur transcription textuelle, résultats de tests psychométriques, objectifs de traitement, résumés de suivi.                                          |
| Catégories de données — techniques                | Journal des accès (auteur, nature de l'action, horodatage, y compris export et suppression), données d'authentification du Praticien, données de connexion.                                                                                                                                                                    |
| Données exclues                                   | La voix du patient n'est jamais enregistrée. Aucune donnée de géolocalisation, aucun identifiant publicitaire, aucune donnée de paiement patient n'est traitée. Le texte des questions adressées à la fonction de recherche n'est pas conservé.                                                                                |
| Base légale du traitement (relevant du Praticien) | Article 6.1.c ou 6.1.f du RGPD selon le cas, combiné à l'article 9.2.h (prise en charge sanitaire ou sociale) et au secret professionnel. La base applicable relève de l'appréciation du Praticien, selon son statut exact, son cadre d'exercice et l'obligation de secret à laquelle il est soumis.                           |
| Durée du traitement                               | Durée de l'abonnement au Service, complétée par les durées de conservation définies à l'article 14 et par les modalités de fin de contrat de l'article 15.                                                                                                                                                                     |
| Fréquence                                         | Traitement continu, au fil de l'utilisation du Service par le Praticien.                                                                                                                                                                                                                                                       |

## Annexe 2 — Sous-traitants ultérieurs autorisés

Liste à jour au **26 août 2026** ; périmètre précisé le **11 septembre 2026**. Toute modification obéit à la procédure de l'article 10.

| Sous-traitant ultérieur   | Prestation confiée                                                                | Localisation                | Données concernées                | Garanties                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|-----------------------------------------------------------------------------------|-----------------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clever Cloud SAS (France) | Hébergement de l'application, de la base de données et des fichiers ; sauvegardes | France — zone certifiée HDS | L'ensemble des Données du Service | Certification n° <b>FR094504</b> délivrée par Bureau Veritas Certification (accréditation COFRAC) selon le <b>référentiel « Hébergeur de données de santé (HDS) — V2 »</b> , valide jusqu'au 19 décembre 2027, couvrant les six activités du référentiel (copie du certificat au dossier de conformité de l'Éditeur, communiquée sur demande) ; contrat d'hébergement de données de santé signé le <b>26 août 2026</b> ; accord de traitement de données de l'hébergeur (clauses contractuelles types de la Commission européenne, décision 2021/915) versé au dossier le 2 septembre 2026 ; chiffrement des données au repos ; base de données dédiée ; sites physiques d'hébergement du certificat, tous situés en France : Telehouse (Paris), nLighten / EXA Infrastructure (Aubervilliers) et OVHCloud (Roubaix, Gravelines), tous couverts par la certification, sans accès aux données depuis un pays tiers à l'Espace économique européen |

| Sous-traitant ultérieur         | Prestation confiée                                                                                                                                     | Localisation     | Données concernées                                                                                                                      | Garanties                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mistral AI SAS (France)         | Transcription de la dictée, structuration du compte rendu, reconnaissance de caractères sur les documents numérisés, résumés et recherche documentaire | Union européenne | Contenu de la dictée du Praticien ; images des documents numérisés ; extraits de dossier soumis aux fonctions de résumé et de recherche | Accord de sous-traitance (article 28) versé au dossier de conformité de l'Éditeur ; mode <b>Zero Data Retention</b> activé au niveau de l'organisation, couvrant les trois interfaces de programmation sans état utilisées par le Service — transcription vocale, génération de texte, reconnaissance optique de caractères — à l'exclusion de toute autre fonction ; utilisation des données pour l'entraînement désactivée et verrouillée ; attestation d'activation conservée au dossier et communiquée sur demande |
| Sendinblue SAS — Brevo (France) | Acheminement des messages électroniques du compte (code de confirmation, réinitialisation du mot de passe)                                             | Union européenne | Adresse électronique et prénom du Praticien uniquement — <b>aucune donnée de patient</b>                                                | Accord de sous-traitance (article 28) ; aucun contenu de dossier transmis                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Périmètre de la présente liste.** N'y figurent que les prestataires qui traitent des Données **pour le compte du Praticien**. En sont exclus, faute d'intervenir sur ces Données :

- **l'hébergeur des fichiers statiques** du site annota.fr et de la version bureau (hébergement mutualisé OVH, France) : il sert le code de l'interface, lequel s'exécute ensuite dans le navigateur du Praticien et n'échange les Données qu'avec l'interface de programmation hébergée chez Clever Cloud. Aucune Donnée ne transite par cet hébergement ni n'y est stockée, aucune requête portant sur un dossier ne lui est adressée ;
- **les prestataires de distribution et de paiement** (Apple, Google, Stripe, RevenueCat) : ils traitent les données d'abonnement du Praticien, traitement pour lequel l'Éditeur agit en qualité de **responsable de traitement** (article 3.3) et non pour le compte du Praticien. Ces traitements sont décrits dans la politique de confidentialité du Service. Aucune donnée de patient ne leur est transmise.

*Cette délimitation a été soumise au conseil juridique et confirmée par lui le 11 septembre 2026.*

Aucun outil de mesure d'audience, de suivi publicitaire ou de remontée automatique d'incidents n'est intégré à l'application mobile.

## Annexe 3 — Mesures techniques et organisationnelles de sécurité

Mesures en vigueur à la date des présentes (**11 septembre 2026**). L'Éditeur les fait évoluer dans les conditions de l'article 8.2.

### 0. Les deux canaux d'accès et ce qui les distingue

Le Service est accessible par deux canaux :

- **l'application mobile** (iOS, Android), installée sur le terminal du Praticien ;
- **la version bureau**, exécutée dans le navigateur d'un ordinateur, sans installation.

Dans les deux cas, les Données sont hébergées et traitées chez l'hébergeur certifié HDS désigné à l'annexe 2 : le canal ne modifie ni la localisation, ni le régime, ni les durées de conservation côté serveur. Il commande en revanche ce qui subsiste, ou non, **sur l'équipement du Praticien** :

|                                                            | Application mobile                                                               | Version bureau (navigateur)                                                                                                         |
|------------------------------------------------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Copie locale du dossier                                    | Oui — chiffrée (AES-256-GCM), sept (7) jours au maximum, purgée à la déconnexion | <b>Aucune</b> — le cache hors-ligne est désactivé ; les Données affichées ne subsistent que dans la mémoire de l'onglet             |
| Jetons de session                                          | Trousseau sécurisé du système (Keychain iOS / Keystore Android)                  | Stockage de session de l'onglet, effacé par le navigateur à sa fermeture ; jamais partagé entre onglets, jamais écrit sur le disque |
| Mémorisation de l'appareil (dispense du code de connexion) | Trente (30) jours glissants                                                      | <b>Sept (7) jours en échéance absolue</b> , et seulement si le Praticien la demande expressément                                    |
| Verrouillage biométrique de l'application                  | Oui                                                                              | Sans objet — la session prend fin à la fermeture de l'onglet                                                                        |
| Fonctionnement hors connexion                              | Oui, en consultation, sur la copie locale chiffrée                               | Non                                                                                                                                 |

**La version bureau expose donc moins de Données que l'application mobile sur l'équipement du Praticien**, l'absence de copie locale étant un choix de conception et non une limitation technique.

### 1. Contrôle d'accès et authentification

- Mot de passe d'au moins douze caractères, stocké sous forme de condensat (bcrypt) ; jamais conservé en clair.
- Confirmation obligatoire de l'adresse électronique à l'inscription ; procédure de réinitialisation à usage unique et à durée limitée, révoquant les sessions ouvertes.
- Jetons de session de courte durée avec rotation des jetons de renouvellement.
- *Application mobile* : verrouillage de l'application par authentification biométrique (reconnaissance faciale ou empreinte) et reverrouillage automatique. *Version bureau* : la fermeture de l'onglet met fin à la session (§ 0).
- Authentification à double facteur du compte praticien par code à usage unique adressé à son adresse électronique, exigée sur tout appareil non reconnu. La mémorisation de l'appareil est limitée à **trente (30) jours glissants sur l'application mobile** et à **sept (7) jours au maximum, en échéance absolue, sur la version bureau** — le Praticien pouvant, sur ce canal, refuser toute mémorisation. Le jeton d'appareil de confiance est une valeur aléatoire opaque qui dispense du seul code de connexion et ne donne par elle-même aucun accès aux Données. Toute réinitialisation du mot de passe révoque les appareils de confiance.

- Limitation du nombre de tentatives d'authentification par origine (protection contre les attaques par force brute) ; codes à usage unique limités en durée et en nombre d'essais.
- Vérification du format du numéro RPPS ou ADELI lorsqu'il est renseigné.

## 2. Chiffrement

- Chiffrement de l'ensemble des communications en transit (TLS).
- Chiffrement des données au repos assuré par l'hébergeur certifié HDS, base de données et fichiers compris.
- *Application mobile* : chiffrement applicatif (AES-256-GCM) de la copie locale sur le terminal du Praticien ; clé conservée dans le trousseau sécurisé du système et détruite à la déconnexion, rendant les résidus illisibles.
- *Version bureau* : aucune copie locale à chiffrer — aucune Donnée n'est écrite sur l'ordinateur. Les jetons de session sont cantonnés au stockage de session de l'onglet, que le navigateur efface à sa fermeture.

## 3. Cloisonnement et minimisation

- Cloisonnement strict des données par praticien, vérifié par des tests automatisés : aucun praticien ne peut accéder aux dossiers d'un autre.
- Suppression automatique de l'enregistrement audio dès la transcription, y compris en cas d'échec du traitement.
- *Application mobile* : copie locale du dossier limitée à sept (7) jours, chiffrée, et purgée à la déconnexion — la clé de chiffrement étant elle-même détruite.
- *Version bureau* : aucune copie locale du dossier. Les exports demandés par le Praticien prennent la forme d'un téléchargement qu'il déclenche et enregistre à l'emplacement de son choix, sous sa responsabilité.
- Absence de conservation du contenu des questions adressées à la fonction de recherche.

## 4. Traçabilité

- Journal des accès horodaté couvrant la consultation, la création, la modification, la suppression et l'export d'un dossier, consultable par le Praticien. Ce journal est tenu côté serveur et enregistre les actions quel que soit le canal utilisé.
- Traçabilité des interventions techniques sur l'environnement de production.

## 5. Intégrité

- Comptes rendus opposables : la validation est expresse et horodatée ; toute correction postérieure à la validation est possible mais horodatée et inscrite au journal des accès, la date de validation d'origine étant conservée.
- Double confirmation exigée pour la suppression d'un dossier.

## 6. Disponibilité et sauvegardes

- Sauvegardes chiffrées de la base de données quotidiennes, rétention de sept (7) jours par défaut (paramétrable auprès de l'hébergeur), au titre de l'activité 6 du référentiel HDS couverte par la certification de l'hébergeur.
- Procédure de restauration testée sur un environnement séparé (test réalisé en septembre 2026), renouvelée périodiquement.

## 7. Développement et exploitation

- Intégration continue avec une base de tests automatisés exécutés à chaque modification.
- Gestion des secrets selon le principe du moindre privilège ; rotation des clés d'accès en cas d'exposition.
- Environnement de préproduction alimenté exclusivement par des données fictives.
- En-têtes de sécurité HTTP, restriction des origines autorisées à interroger l'interface de programmation, liste blanche des types de fichiers acceptés à l'import et au téléchargement.

- Les fichiers de la version bureau (code de l'interface) sont servis depuis un hébergement distinct de celui des Données ; ils ne contiennent aucune Donnée, et l'interface n'échange les Données qu'avec l'interface de programmation hébergée chez l'hébergeur certifié HDS, au moyen d'une liste restrictive d'origines autorisées.
- Revue de sécurité interne documentée (référentiels OWASP API Security Top 10, ASVS et MASVS) réalisée le 5 septembre 2026, constats corrigés le jour même ; **test d'intrusion par un prestataire indépendant dans les douze (12) mois suivant l'ouverture du Service aux données réelles, puis annuel (article 8.3).**

## 8. Organisation

- Engagement de confidentialité des personnes autorisées à intervenir sur le Service.
- Sélection des sous-traitants ultérieurs sur des critères incluant la localisation européenne, la certification HDS pour l'hébergement et l'absence de réutilisation des données.
- Analyse d'impact relative à la protection des données réalisée pour le Service et tenue à disposition du Praticien.

## Annexe 4 — Contenu de la notification d'une violation de données

---

La notification adressée par l'Éditeur au Praticien comporte au minimum les éléments suivants, dans la mesure où ils sont disponibles au moment de la notification :

- la description de la nature de la violation, sa date ou sa période de survenance et la date à laquelle l'Éditeur en a eu connaissance ;
- les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements concernés ;
- la précision des dossiers ou des comptes affectés, lorsqu'elle peut être établie ;
- les conséquences probables de la violation ;
- les mesures prises ou proposées pour remédier à la violation et en atténuer les effets ;
- le nom et les coordonnées du point de contact auprès duquel des informations complémentaires peuvent être obtenues ;
- les éléments utiles au Praticien pour apprécier la nécessité d'une notification à l'autorité de contrôle et d'une communication aux personnes concernées. Lorsque ces informations ne peuvent être communiquées en une seule fois, elles sont transmises de manière échelonnée, sans retard indu, et un point de situation est adressé au Praticien au moins tous les **trois (3) jours** jusqu'à la clôture de l'incident (article 13.2).