

# Accord de traitement des données

Clauses contractuelles types (UE) 2021/915 + annexes DentalSuite

---

Version du 1er octobre 2026 (révision 4) — applicable aux professionnels de santé  
Publié le 26 septembre 2026 · <https://dentalsuite.fr/dpa/2026-10-01-r4.html>

---

## Note sur ce document

Le corps des clauses (Sections I à III) reprend le texte officiel de la Commission, tel que fourni depuis EUR-Lex. Deux adaptations ont été faites, autorisées par le modèle : (1) parmi les mentions « règlement 2016/679 et/ou 2018/1725 », seul le règlement 2016/679 (RGPD) a été retenu — le règlement 2018/1725 vise les institutions de l'UE, non ZB Solutions ; (2) les options ont été fixées : clause 7.7 = Option 2 (autorisation générale), clause 8 = Option 1 (article 32 RGPD). Le champ de durée laissé ouvert par le modèle à la clause 7.7 a été renseigné à « un (1) mois ».

Les quatre annexes (I à IV) sont l'apport rédigé pour DentalSuite. Aucune clause du corps n'a été modifiée sur le fond ; seuls les choix prévus par le modèle ont été opérés.

## CLAUSES CONTRACTUELLES TYPES

### SECTION I

#### Clause 1 · Objet et champ d'application

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

#### Clause 2 · Invariabilité des clauses

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

### **Clause 3 · Interprétation**

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

### **Clause 4 · Hiérarchie**

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

### **Clause 5 · Clause d'amarrage (facultative)**

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

## **SECTION II — OBLIGATIONS DES PARTIES**

### **Clause 6 · Description du ou des traitements**

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'annexe II.

### **Clause 7 · Obligations des parties**

## **7.1. Instructions**

a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

## **7.2. Limitation de la finalité**

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

## **7.3. Durée du traitement des données à caractère personnel**

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

## **7.4. Sécurité du traitement**

a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.

b) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

## **7.5. Données sensibles**

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

## **7.6. Documentation et conformité**

a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

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

### **7.7. Recours à des sous-traitants ultérieurs**

DentalSuite retient l'option 2 ci-dessous ; l'option 1 (autorisation spécifique préalable) du texte officiel est écartée.

- a) **OPTION 2 : AUTORISATION ÉCRITE GÉNÉRALE** : le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins un (1) mois à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.
- b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679.
- c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.
- d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
- e) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

## 7.8. Transferts internationaux

a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679.

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

## Clause 8 · Assistance au responsable du traitement

a) Le sous-traitant informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.

b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.

c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

- 1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d'impact relative à la protection des données ») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;
- 2) l'obligation de consulter l'autorité de contrôle compétente préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
- 3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;
- 4) les obligations prévues à l'article 32 du règlement (UE) 2016/679.

d) Les parties définissent à l'annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

## Clause 9 · Notification de violations de données à caractère personnel

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

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

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

a) aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques) ;

b) aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins :

- 1) la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- 2) les conséquences probables de la violation de données à caractère personnel ;
- 3) les mesures prises ou les mesures que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

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

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

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

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

a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;

b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;

c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

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

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

## SECTION III — DISPOSITIONS FINALES

### Clause 10 · Non-respect des clauses et résiliation

a) Sans préjudice des dispositions du règlement (UE) 2016/679, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

b) Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

- 1) le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
- 2) le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 ;
- 3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679.

c) Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.

d) À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

— Fin du corps des clauses contractuelles types (texte officiel, options DentalSuite sélectionnées). —

## ANNEXES — RENSEIGNÉES POUR DENTALSUITE

### ANNEXE I — Liste des parties

#### Responsable du traitement

Le cabinet client souscripteur du service DentalSuite. Identité renseignée à la souscription :

- Nom / raison sociale : celle du cabinet souscripteur, telle qu'enregistrée dans son compte client et consultable depuis l'espace Administration du Service.
- Adresse : celle du cabinet souscripteur, telle qu'enregistrée dans son compte client et consultable depuis l'espace Administration du Service.

Nom, fonction et coordonnées de la personne de contact : ceux du titulaire du compte du cabinet

souscripteur, tels qu'enregistrés dans son compte client et consultables depuis l'espace Administration du Service.

- Signature et date d'adhésion : acceptation horodatée à la souscription.

### **Sous-traitant**

- Nom : ZB Solutions (SASU)
- Adresse : 62 avenue de Vallauris, 06400 Cannes

Nom, fonction et coordonnées de la personne de contact : Mme Yaël Zerbib, Présidente —  
contact@dentalsuite.fr

- Signature et date d'adhésion : adhésion effective à la date de mise à disposition du Service au Client, horodatée dans le Service.

Aucun délégué à la protection des données n'est désigné à ce jour.

## **ANNEXE II — Description du traitement**

### **Catégories de personnes concernées**

- les patients du cabinet ;
- les membres du personnel et utilisateurs du cabinet.

### **Catégories de données à caractère personnel traitées**

- données d'identification et administratives des patients : nom, prénom, date de naissance, coordonnées de contact, et identifiant de synchronisation de l'agenda externe ;
- données relatives aux utilisateurs (identité professionnelle, identifiants de connexion, données de journalisation).

### **Données sensibles traitées, limitations et garanties appliquées**

Le traitement porte sur des données concernant la santé, catégorie particulière au sens de l'article 9 du RGPD : dates de consultation et de dernière visite, indicateurs de suivi orthodontique, actes prothétiques, poses d'implants, traitements d'orthodontie, devis de soins, rendez-vous et leurs motifs. Conformément à la clause 7.5, garanties appliquées : limitation stricte de la finalité ; restriction des accès selon le rôle de chaque utilisateur ; tenue d'un registre des opérations (journalisation horodatée et nominative des créations, modifications, suppressions et archivages) ; astreinte au secret professionnel ; hébergement exclusif en UE auprès d'un hébergeur certifié HDS ; interdiction de tout transfert de données de santé hors UE.

L'interdiction de transfert hors UE porte sur les données de santé des patients. Les sous-traitants ultérieurs situés hors UE (voir annexe IV) n'ont accès à aucune donnée de santé et interviennent exclusivement sur des traitements techniques ou commerciaux périphériques, encadrés par les clauses contractuelles types.

### **Nature du traitement**

Hébergement, stockage, organisation, consultation et mise à disposition des données, aux seules fins de la gestion et de l'organisation de l'activité du cabinet.

### **Finalités**

Fournir au cabinet un logiciel de gestion : stocks et prothèses, rendez-vous, devis, orthodontie, avis patients,

fonctions transverses.

## **Durée du traitement**

Pendant toute la durée de l'abonnement, y compris, le cas échéant, la période transitoire de changement de fournisseur, puis pendant la période de récupération de trente (30) jours calendaires prévue aux articles 9.3 et 9.4 des CGV. Suppression des systèmes actifs au terme de cette période ou, sur demande du responsable du traitement, dès l'exécution de celle-ci ; effacement complet, sauvegardes comprises, dans un délai maximal de douze (12) mois après cette suppression (aligné sur les CGV, article 11.3), sans préjudice des obligations légales de conservation incombant au cabinet.

## **Traitement par les sous-traitants ultérieurs (objet, nature, durée)**

Scalingo (hébergement HDS) : hébergement de l'infrastructure et de la base de données, pour toute la durée de l'abonnement. Autres sous-traitants ultérieurs éventuels : voir annexe IV.

## **ANNEXE III — Mesures techniques et organisationnelles**

Hébergement et sécurité physique : Scalingo, certifié HDS, région osc-fr1 (France / UE).

Cloisonnement multi-tenant : chaque cabinet client dispose d'un identifiant propre. Le cloisonnement des données entre cabinets est imposé par la base de données elle-même et non par le code applicatif : les tables contenant les données des patients et des soins — soixante-quinze (75) tables sur les quatre-vingt-sept (87) que compte le schéma applicatif — sont soumises au mécanisme Row Level Security de PostgreSQL en mode FORCE, assorti d'une politique n'autorisant l'accès qu'aux lignes du cabinet courant. Les autres ne portent aucune donnée de patient : fiche administrative du cabinet, jetons de liens à usage unique, tables de référence communes et tables techniques, auxquelles le rôle applicatif n'a pour partie aucun droit. Le rôle utilisé par l'application ne dispose d'aucun privilège de contournement de ces politiques. L'identifiant du cabinet est établi par le serveur à partir du jeton d'authentification signé, jamais transmis par le poste client ; en son absence, la requête est refusée. Deux mécanismes strictement délimités existent, nécessaires au fonctionnement de l'authentification et des liens à usage unique. Le premier est une règle de la base qui n'autorise la recherche d'un compte par son identifiant que tant qu'aucun cabinet n'est établi. Le second est la résolution d'un jeton de lien public, effectuée par une connexion technique dédiée sur les seules tables de jetons. Aucun des deux ne donne accès aux données de patients ; l'un et l'autre sont bornés à la résolution d'un identifiant ou d'un jeton.

Mots de passe : aucun mot de passe n'est conservé. Seule une empreinte est calculée au moyen d'Argon2id (version 19), avec un coût mémoire de 64 Mio, trois itérations et un parallélisme de quatre. Un sel unique est généré pour chaque empreinte. Une longueur minimale de dix caractères est exigée. La vérification s'effectue par recalcul, sans jamais reconstituer le mot de passe.

Reconnexion rapide : sur un poste préalablement déclaré de confiance lors d'une connexion par mot de passe, l'utilisateur peut rouvrir une session au moyen d'un code personnel à quatre chiffres. Cette reconnexion requiert un identifiant d'appareil aléatoire conservé sur le poste et la connaissance du code. La session ainsi ouverte ne permet pas les opérations sensibles, qui exigent une nouvelle saisie du mot de passe. Le code est soumis au même mécanisme de hachage que les mots de passe. Cinq tentatives infructueuses le verrouillent quinze minutes, l'accès par mot de passe demeurant disponible. Les postes de confiance sont révoqués à tout changement ou réinitialisation du mot de passe, ainsi qu'à la désactivation du compte ; l'utilisateur consulte et révoque à tout moment la liste de ses postes enregistrés.

Protection en transmission et au stockage : les échanges entre les postes des utilisateurs et le Service sont chiffrés en transit au moyen du protocole TLS. Les données sont hébergées au sein de l'Union européenne auprès d'un hébergeur certifié Hébergeur de Données de Santé, dont les mesures de protection physique et

de chiffrement des supports relèvent de sa propre certification.

**Journalisation** : les créations, modifications, suppressions et archivages de données font l'objet d'un enregistrement horodaté et nominatif, conservé dans le Service et non modifiable par l'application. L'export complet des données du cabinet y est également enregistré.

**Disponibilité et résilience** : des sauvegardes régulières de la base de données sont assurées par l'hébergeur certifié HDS, qui les conserve jusqu'à douze (12) mois selon une rotation qu'il détermine. Le Sous-traitant mettra en place une vérification documentée de leur restauration.

**Minimisation et conservation limitée** : données strictement nécessaires ; les durées applicables en cours de contrat figurent dans la politique de conservation des données ; en fin de contrat, suppression des systèmes actifs au terme de la période de récupération de trente (30) jours calendaires, ou plus tôt sur demande, et effacement complet, sauvegardes comprises, au plus tard douze (12) mois après cette suppression.

**Accès de l'Éditeur** : l'administration du Service repose sur un compte unique, distinct des comptes de cabinet — il ne partage ni la table des comptes, ni la clé de signature des sessions, ni les adresses d'accès. Il est protégé par une double authentification par code temporaire, active. Son périmètre est limité aux données d'abonnement et de facturation — identité du cabinet, formule, échéances, consommation d'envois — à l'exclusion de toute donnée de patient ou de soin, et cette limite est imposée par la base de données elle-même. Chacun de ses accès est journalisé dans un registre distinct, en ajout seul.

### **Mesures d'assistance au responsable (clauses 8, 9 et 10)**

Le Sous-traitant met à disposition les fonctionnalités d'export et de rectification permettant au Responsable de répondre aux demandes des personnes concernées. **Effacement d'un patient** : l'effacement d'un patient est exécuté par le Sous-traitant sur demande écrite du Responsable adressée à [contact@dentalsuite.fr](mailto:contact@dentalsuite.fr), dans un délai de dix (10) jours ouvrés. Il retire l'identité du patient et vide les textes saisis librement le concernant, en conservant le rattachement des actes passés et les valeurs choisies dans des listes fermées. Sont seuls conservés : une trace de l'opération, sans identité (auteur, date et identifiant interne du patient) ; l'identifiant de synchronisation de l'agenda externe, afin qu'un import ultérieur ne recrée pas la fiche ; des empreintes de l'adresse électronique, qui ne permettent pas de la lire, nécessaires au respect d'une opposition et à la maîtrise de la fréquence des envois (prévention des envois en double ou trop rapprochés, exclusion des patients déjà sollicités, suivi des relances de contrôle). En cas de violation, le Sous-traitant communique au Responsable les éléments listés à la clause 9 (nature, point de contact, conséquences, mesures).

**Fin du contrat (clause 10, point d))** : le Responsable choisit entre la restitution de ses données, au moyen de l'export en libre-service disponible pendant la période de récupération, suivie de leur suppression, et leur suppression sans attendre le terme de cette période, sur demande adressée à [contact@dentalsuite.fr](mailto:contact@dentalsuite.fr). Dans les deux cas, le Sous-traitant certifie la suppression par une attestation datée adressée par courrier électronique au titulaire du compte, indiquant la date de suppression des systèmes actifs et la date à laquelle l'effacement des sauvegardes sera acquis.

**Communications aux patients** : à compter de la date d'effet de la résiliation, le Sous-traitant n'adresse plus aucune communication aux patients du Responsable via le Service, et les liens publics qui leur ont été transmis ne donnent plus accès aux formulaires correspondants, à l'exception du lien de désinscription, qui demeure opérant pendant sa durée de validité.

**Opposition des patients** : les messages de relance de contrôle adressés aux patients via le Service comportent un lien de désinscription. La désinscription est enregistrée sous la forme d'une empreinte de l'adresse électronique. L'ouverture d'un lien contenu dans un message n'enregistre aucune demande du patient sans confirmation expresse de sa part.

## ANNEXE IV — Liste des sous-traitants ultérieurs

Note officielle : cette annexe est formellement requise en cas d'autorisation spécifique (option 1).

DentalSuite ayant retenu l'OPTION 2 (autorisation générale), la liste ci-dessous constitue la « liste convenue » au sens de l'option 2 : tenue à jour, toute modification faisant l'objet d'une information préalable écrite un mois à l'avance avec droit d'opposition.

Pour chaque sous-traitant ultérieur : nom, description du traitement (objet, nature), localisation.

- Scalingo SAS — hébergement de l'infrastructure et de la base de données. Localisation : France (UE), certifié HDS.
- Brevo (Sendinblue SAS) — acheminement des messages électroniques envoyés par le cabinet depuis le Service (sollicitations d'avis, relances de devis, rappels de rendez-vous, courriers d'activation). Localisation : France (UE), hébergeur non certifié HDS. Données transmises : nom, prénom et adresse électronique du destinataire, nom du cabinet et du praticien, date d'un rendez-vous ou d'un devis. Aucune donnée clinique, aucun montant, aucun document médical ne lui est transmis.
- Stripe Payments Europe, Ltd — traitement des paiements. Localisation : Irlande (UE).
- Functional Software, Inc. d/b/a Sentry, société de droit américain — supervision technique et journalisation des erreurs applicatives. Les événements d'erreur sont hébergés dans l'Union européenne, à Francfort (Allemagne), avec sauvegardes dans l'Union. Les données de compte permettant d'identifier la région de rattachement de l'organisation sont susceptibles d'être répliquées hors de l'Union ; aucune donnée de patient n'y figure. Aucune donnée de santé n'est transmise : les messages d'erreur sont expurgés à la source selon une liste blanche de champs autorisés. Rétention des événements : trente (30) jours, durée appliquée par le prestataire selon la formule souscrite et susceptible d'évoluer avec elle. Transferts encadrés par les clauses contractuelles types (art. 46, §2, RGPD).
- Netlify, Inc. — hébergement des fichiers du site vitrine et de l'application du cabinet (pages, feuilles de style et programmes exécutés par le navigateur). Localisation : États-Unis. Aucune donnée applicative ni donnée de santé n'y est stockée ni n'y transite : les échanges de données se font directement entre le navigateur de l'utilisateur et l'hébergeur certifié HDS. Netlify a en revanche connaissance de l'adresse IP des visiteurs et des utilisateurs, par la nature même d'un service de distribution de fichiers. Transfert encadré par les clauses contractuelles types (art. 46, §2, RGPD).
- Calendly, LLC — prise de rendez-vous commerciale (prospection). Localisation : États-Unis. N'a accès à aucune donnée de patient ni donnée applicative ; traite uniquement les coordonnées des prospects sollicitant une démonstration. Transfert encadré par les clauses contractuelles types (art. 46, §2, RGPD).

DentalSuite — édité et distribué par ZB Solutions