



## CONDITIONS PARTICULIERES DE FOURNITURE DE SERVICES PROFESSIONNELS

Ces Conditions particulières de services sont applicables, outre les **CONDITIONS GENERALES DE LICENCE / MAINTENANCE ZENLOCASSUR** (les « Conditions générales »), dès lors que ZENLOCASSUR réalise des prestations de services professionnels.

### ARTICLE 1. DESCRIPTION GÉNÉRALE

Les « Services Professionnels » peuvent inclure les services suivants fournis par ZENLOCASSUR : services de mise en œuvre (set-up), conseil, gestion de projet, formation et autres services connexes, prestations non comprises dans les services de maintenance définies dans les Conditions générales.

### ARTICLE 2. EXIGENCES RELATIVES A LA FOURNITURE DU SERVICE

Le Client s'engage à :

- engager des ressources suffisantes pour le projet et veiller à ce que le personnel clé du client soit disponible à tout moment pour fournir à ZENLOCASSUR les informations et les instructions nécessaires, y compris le remplacement en temps utile de ce personnel ;
- fournir toutes les informations raisonnablement demandées par ZENLOCASSUR en temps utile ;
- s'assurer qu'il se conforme aux hypothèses et à ses obligations telles que définies dans le descriptif de Service applicable ;
- confirmer son acceptation de tout élément ou objectif proposé par ZENLOCASSUR pour acceptation, si cet élément répond aux critères convenus (tels que définis dans le descriptif de Service applicable) ; et
- tenir ZENLOCASSUR informée de tout développement susceptible d'affecter la réalisation d'un projet.

### ARTICLE 3. LIVRAISON DU SERVICE

ZENLOCASSUR fournira les Services Professionnels dans tous les aspects matériels tels que décrits dans le descriptif de Service applicable.

Les Services Professionnels seront fournis les jours ouvrables, sauf accord contraire écrit entre les Parties.

Les Services commenceront à la date et se poursuivront pendant la durée fixée dans le descriptif de Service applicable ou comme convenu par les Parties.

Les délais de fourniture les Services Professionnels indiqués dans le cahier des charges ou convenues entre les Parties ne sont que des estimations.

Sauf accord contraire, les Services Professionnels seront fournis à distance. Pour que les Services Professionnels soient fournis sur le site du Client, ce dernier doit s'assurer que ZENLOCASSUR dispose d'un accès complet aux installations, équipements et systèmes lui permettant de fournir le service.

A condition que ZENLOCASSUR reste responsable de la fourniture des Services Professionnels elle sera autorisée à sous-traiter la fourniture des Services Professionnels

### ARTICLE 4. DÉLAI ET PAIEMENT

Sauf indication contraire dans une commande :

- Les montants spécifiés dans une commande ne sont que des estimations et ZENLOCASSUR facturera le Client pour les

services sur la base du temps réellement passé par ZENLOCASSUR ;

- les Services Professionnels et toutes les dépenses seront payables en temps et en matériel (jour ouvrable), mensuellement à terme échu, sur la base des tarifs en vigueur de ZENLOCASSUR ;
- des frais supplémentaires peuvent s'appliquer si les Services Professionnels sont fournis en dehors des jours ouvrables ;
- ZENLOCASSUR facturera une journée entière pour toute partie de journée travaillée ; et
- les dépenses sont encourues par le personnel de ZENLOCASSUR conformément à la politique de dépenses de ZENLOCASSUR en vigueur à ce moment-là (qui peut être fournie sur demande).

### ARTICLE 5. MODIFICATION DES SERVICES PROFESSIONNELS

Si des changements sont convenus entre les Parties ou sont nécessaires, les Parties suivront le processus de contrôle du changement défini dans le descriptif de Service applicable. Si aucune procédure de contrôle des changements n'est définie dans le cahier des charges, les parties coopéreront de bonne foi pour convenir des changements nécessaires.

Les Parties coopèrent également de bonne foi pour convenir de la modification des redevances applicables à la suite des modifications requises. Si les Parties ne parviennent pas à se mettre d'accord, ZENLOCASSUR aura le droit de facturer les Services Professionnels aux tarifs en vigueur.

Si les Parties ne parviennent pas à se mettre d'accord sur les changements à apporter au cahier des charges ou aux prix applicables, ZENLOCASSUR aura le droit soit (i) de continuer à fournir les Services Professionnels sur la base du cahier des charges ou du descriptif de Services Professionnels existant, soit (ii) de cesser le travail et de se faire payer de tous les coûts ou dépenses jusqu'à cette date.

### ARTICLE 6. REPROGRAMMATION ET ANNULATION

Si les Parties ont convenu de dates spécifiques pour la fourniture du Service et que le Client annule ou reporte une partie ou la totalité du Service ou que ZENLOCASSUR n'est pas en mesure de fournir le Service en raison d'actes ou d'omissions du client, ZENLOCASSUR sera en droit de facturer au client :

- (i) 50% des frais concernés si l'avis d'annulation ou de report est reçu par ZENLOCASSUR entre six (6) et dix (10) jours ouvrables avant la date convenue pour la fourniture du service ; et
- (ii) 100 % des frais concernés si la notification d'annulation / de report est reçue par ZENLOCASSUR cinq (5) jours ouvrables ou moins avant la date convenue pour la livraison du Service.

En outre, ZENLOCASSUR a le droit de facturer au Client tous les frais encourus du fait de l'annulation/du report.

ZENLOCASSUR fera tout son possible pour redéployer le personnel concerné afin d'atténuer la responsabilité du client en vertu de la présente clause.

### ARTICLE 7. TESTS D'ACCEPTATION PAR L'UTILISATEUR

Le Client est responsable de la mise en place et de la réalisation des tests d'acceptation par l'utilisateur pour les Services Professionnels faisant partie d'un Projet. Les Parties suivront les procédures de tests d'acceptation définies dans le cahier des charges ou dans d'autres

documents fournis au Client. Si aucune procédure de test d'acceptation n'est fournie au Client, ce dernier doit effectuer et achever ces tests dès qu'il est raisonnablement possible de le faire après avoir été informé que les services ou les produits livrables sont prêts à être testés.

## ARTICLE 8. SIGNATURE ELECTRONIQUE

Les Parties s'engagent à signer électroniquement le Contrat conformément aux dispositions des Lois et Règlements relatifs à la signature électronique, par l'intermédiaire d'un prestataire qui assurera la sécurité et l'intégrité de la version numérique du présent Contrat conformément aux Lois et Règlements relatifs à la signature électronique.

### ANNEXE RGPD

Le Client agissant en qualité de responsable de traitement :

(Ci-après « le Client »), et

ZENLOCASSUR agissant en qualité de sous-traitant :

Adresse : 14 rue du X septembre, L-2550 Luxembourg, Luxembourg

Fonction et coordonnées de la personne de contact : Délégué à la Protection des Données, [privacy@zenlocassur.com](mailto:privacy@zenlocassur.com)

(Ci-après « ZENLOCASSUR »), ensemble désignée « les Parties ».

Les présentes clauses visent à définir les obligations des Parties concernant la protection des données, et font partie intégrante Conditions particulières de prestations de services professionnels.

Les Parties s'engagent à garantir la conformité de la collecte et du traitement des Données à caractère personnel avec le 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 (règlement générale sur la protection des données, ci-après « RGPD » ou la « Réglementation en vigueur »).

#### Article 1 – Définitions

Les termes « Autorité de contrôle », « Délégué à la Protection des Données », « Données sensibles », « Données à caractère personnel », « Personne concernée », « Responsable de traitement », « Sous-traitant », « Traitement », « Transfert », et « Violation de données » sont définis à l'article 4 du RGPD.

#### Article 2 – Description du ou des traitements

Les détails des opérations de traitement réalisées par le Prestataire, 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 Client, sont précisés à l'annexe I.

Le Prestataire traite les Données à caractère personnel uniquement pour la ou les finalités décrites, sauf instruction complémentaire du Client.

#### Article 3 – Obligations des parties

##### 3.1 Instructions

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

Si une instruction donnée par le Client constitue une violation de la Réglementation en vigueur, le Prestataire en informe immédiatement le Client.

Si le Prestataire est tenu de procéder à un Transfert de Données, il informe immédiatement le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Chaque Partie s'engage à prendre toutes les mesures appropriées afin que la signature électronique du présent Contrat soit apposée par son représentant ou toute autre personne dûment autorisée aux fins des présentes.

Chaque Partie reconnaît et s'engage par les présentes à ce que la signature du Contrat via le procédé électronique susmentionné s'effectue en pleine connaissance de la technologie mise en œuvre, de ses conditions d'utilisation et des Lois et Règlements relatifs à la signature électronique et, par conséquent, renonce irrévocablement et inconditionnellement à son droit d'intenter toute action en justice et/ou réclamation, découlant directement ou indirectement de la fiabilité dudit procédé de signature électronique et/ou des preuves de son intention de conclure le Contrat à cet égard.

Le Prestataire s'engage à ne pas utiliser les Données pour son propre compte, ou pour le compte d'un tiers, ni à les communiquer en contradiction avec les instructions données par le Client.

##### 3.2 Sécurité du traitement

Le Prestataire met en œuvre les mesures techniques et organisationnelles précisées dans sa Politique de sécurité des traitements, jointe aux présentes clauses, 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.

Le Prestataire 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 Prestataire veille à ce que les personnes autorisées à traiter les Données à caractère personnel soient soumises à une clause de confidentialité.

Si le ou les traitements décrits en annexe I portent sur des Données sensibles. A ce titre, le Prestataire applique des limitations spécifiques et/ou des garanties complémentaires.

Dans le cadre des Prestations prévues dans le Devis, le Prestataire n'accède pas aux données du Client.

En cas d'accès aux Données du Client dans le cadre Prestations prévues dans le Devis, le Prestataire intervient uniquement sur sollicitation et autorisation préalable du Client. Des registres seront établis sous les responsabilités respectives des Parties, mentionnant les dates et natures détaillées des interventions de maintenance à distance ainsi que les noms de leurs auteurs.

Lorsque le Prestataire accède au système informatique du Client, il s'engage à ce que son personnel y accède conformément aux règles d'habilitation d'accès du Client.

##### 3.3 Documentation et conformité

Les Parties doivent pouvoir démontrer leur conformité avec les présentes clauses.

Le Prestataire traite de manière rapide et adéquate les demandes du Client concernant le traitement des Données conformément aux présentes clauses.

Le Prestataire met à disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement de la Réglementation en vigueur.

A la demande du Client, le Prestataire permet la réalisation d'audits des activités du traitement couvert par les présentes clauses, à intervalles raisonnables ou en présence d'indices de non-conformité, sous réserve d'un préavis de 20 jours.

Le Client 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.

Les Parties mettent à disposition de l'Autorité de contrôle, dès que celle-ci en fait la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

Le Prestataire a désigné un Délégué à la Protection des Données, dont les coordonnées sont les suivantes : [privacy@zenlocassur.com](mailto:privacy@zenlocassur.com)

Le Prestataire s'engage à tenir un registre des traitements conforme à l'article 30 2. du RGPD, et à le mettre à disposition sur demande du Client.

### 3.4 Droits des Personnes concernées

Il est convenu que le Client a l'obligation d'informer les Personnes concernées par le traitement de leurs Données conformément aux articles 13 et 14 du RGPD.

Le Client veille à définir les bases légales du ou des traitements, objets du Contrat.

### 3.5 Recours à un sous-traitant ultérieur

Le Prestataire dispose d'une autorisation générale du Client pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue laquelle sera annexée aux présentes clauses, avec les informations suivantes : Nom ; Description du traitement (objet, nature et durée). Le Prestataire informe spécifiquement par écrit le Client de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins un mois à l'avance afin de permettre au Client de prendre le temps nécessaire pour s'opposer au recrutement du sous-traitant ultérieur. Le Prestataire communique dans le même temps les informations nécessaires pour permettre au Client de s'opposer si nécessaire.

Le Client peut s'opposer au recrutement d'un sous-traitant ultérieur, sous réserve d'invoquer un motif légitime. Le Client est informé qu'en cas d'opposition, le Prestataire prendra les mesures nécessaires pour assurer la continuité du Contrat sans le recours du sous-traitant ultérieur. Si la continuité du Contrat ne peut pas être assurée, les Parties seront en droit de résilier le Contrat.

En cas de recours à un sous-traitant ultérieur, le Prestataire s'engage à encadrer ces relations par un contrat qui impose au sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles imposées au Prestataire en vertu des présentes clauses. Le Prestataire veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et de la Réglementation en vigueur.

Sur demande du Client, le Prestataire communique une copie du contrat signé avec le sous-traitant ultérieur. Le Prestataire est autorisé à ne pas communiquer certaines informations du contrat afin de protéger des secrets d'affaires, des informations confidentielles ou des données à caractère personnel.

Le Prestataire est seul responsable de l'exécution des obligations du sous-traitant ultérieur. Il en informe le Client en cas de tout manquement du sous-traitant ultérieur de ces obligations contractuelles.

### 3.6 Transfert de données hors UE

Les transferts de données en dehors de l'Union européenne ne sont effectués par le Prestataire que sur la base d'instructions documentées du Client. Le Prestataire est autorisé à réaliser un transfert de données afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le Prestataire est soumis. Tout transfert de données s'effectue conformément au chapitre V du RGPD.

Les transferts de données en dehors de l'Union européenne ne sont effectués par le sous-traitant ultérieur que si les dispositions du chapitre V du RGPD sont respectées par le Prestataire et le sous-traitant ultérieur.

## Article 4 – Assistance du Prestataire au Client

Le Prestataire aide le Client dans son obligation de réaliser une analyse d'impact relative à la protection des données, si un traitement est susceptible de présenter un risque élevé pour les droits et libertés des Personnes concernées.

Lorsque le Prestataire constate que des données sont inexactes et devenues obsolètes, il en informe le Client.

## Article 5 – Notification des violations de données

En cas de Violation de Données à caractère personnel, le Prestataire coopère avec le Client en vertu de la Réglementation en vigueur et notamment des articles 33 (notification d'une Violation de données à l'Autorité de contrôle) et 34 (communication d'une Violation de données aux Personnes concernées) du RGPD.

### 5.1 Violation de données en rapport avec des données traitées par le Client

Dans ce cas, le Prestataire prête assistance au Client, aux fins de la notification de la violation de données à l'Autorité de contrôle et de l'obtention des informations nécessaire, dans les meilleurs délais après que le Client en a eu connaissance.

Si la Violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés des Personnes concernées, le Prestataire prête assistance au Client de l'obligation qui lui incombe de communiquer dans les meilleurs délais de la violation auprès des Personnes concernées.

### 5.2 Violation de données en rapport avec des données traitées par le Prestataire

Dans ce cas, le Prestataire informe le Client dans les meilleurs délais, et au plus tard 72h, après en avoir pris connaissance, par courrier électronique à l'adresse communiquée par le Client lors de la souscription aux services du Prestataire.

Le Prestataire s'engage à fournir au Client toutes les informations nécessaires pour documenter une Violation de données conformément à la Réglementation en vigueur et notamment aux articles 33 et 34 du RGPD.

## Article 6 – Non-respect des clauses et résiliation

En cas de manquement du Prestataire aux obligations qui lui incombent en vertu des présentes clauses, le Client peut demander au Prestataire de suspendre le traitement de Données jusqu'à que le Prestataire se conforme de nouveau aux présentes clauses, ou jusqu'à la résiliation du Contrat. Le Prestataire informe dans les meilleurs délais le Client s'il n'est pas en mesure de se conformer aux présentes clauses.

Le Client est en droit de résilier le Contrat si :

- Le traitement de Données effectué par le Prestataire a été suspendu par le Client ;
- 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 du traitement ;
- Le Prestataire est en violation grave ou persistance des présentes clauses ou des obligations qui lui incombent en vertu de la Réglementation en vigueur ;
- Le Prestataire ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'Autorité de contrôle.
- Le Client s'oppose au recours d'un sous-traitant ultérieur pour des motifs légitimes, et que la continuité du Contrat ne peut pas être assurée.

Le Prestataire est en droit de résilier le Contrat si, après avoir informé le Client, que des instructions données enfreignent la Réglementation en vigueur et qu'à ce titre, le Client insiste pour que ses instructions soient suivies.

Les prestations objet du Contrat n'impliquent aucune conservation des Données personnelles par le Prestataire, lequel aura accès aux données du Client uniquement le temps nécessaire à la prestation.

Le Prestataire veille à se conformer aux présentes clauses pendant toute la durée de la prestation.

Les présentes clauses entrent en vigueur à compter de la signature du Contrat.

*Les présentes clauses ont la même durée d'exécution que le Contrat.*

## **Annexe I – Description du traitement**

### **Catégorie de personnes concernées dont les Données sont traitées :**

- *Utilisateurs*
- *Assurés*
- *Prospects*

### **Catégories de Données traitées :**

- *Données d'identification*
- *Vie personnelle*
- *Vie professionnelle*
- *Informations économiques et financières*
- *Données de connexion*

### **Données sensibles traitées, garanties et mesures supplémentaires :**

- *Numéro de sécurité sociale*
- *Données de santé*

### **Nature du traitement**

- *En fonction des prestations prévues dans le Devis, notamment : organisation, structuration, consultation*

### **Finalité(s) pour laquelle (lesquelles) les Données sont traitées pour le compte du Client :**

- *Prestations définies dans le Devis (Services professionnels : services de mise en œuvre (set-up), conseil, gestion de projet, formation et autres services connexes)*
- 

### **Durée du traitement :**

- *Durée nécessaire à la réalisation des Prestations*

## **Annexe II – Liste des sous-traitants ultérieurs**

1. *Nom : AXOM GROUPE*

*SARL inscrite au RCS de BEAUVAIS sous le numéro 814499539*

*Adresse : 22 rue des Haies de Fay – CLERMONT - France*

*Description du traitement : prestations informatiques*

2. *Nom : KOOLAB*

*SAS inscrite au RCS de BOBIGNY sous le numéro 909392177*

*Adresse : 1 B avenue du château – VINCENNES - France*

*Description du traitement : prestations informatiques*

3. *Nom : ADJUVOO*

*SAS inscrite au RCS de PARIS sous le numéro 898001029*

*Adresse : 83 boulevard Auriol – PARIS – France*

*Description du traitement : prestations informatiques et de gestion de projets*

## Annexe III – Politique de sécurité de ZENLOCASSUR

Cette politique vise à informer sur les mesures de sécurité techniques et organisationnelles mises en œuvre par la société pour garantir la protection des données personnelles et des systèmes d'information. La première partie détaille les mesures applicables à l'ensemble de l'organisation et la seconde partie, les mesures spécifiques applicables au logiciel et aux services associés.

### MESURES DE SÉCURITÉ GÉNÉRALES

1. **Authentification des utilisateurs et contrôle des accès logiques :**
  - Login et mot de passe unique attribués à chaque utilisateur.
  - Utilisation d'un générateur de mots de passe robustes.
  - Renouvellement des mots de passe une fois par mois.
  - Double authentification activée sur Office 365.
  - Règles renforcées pour les mots de passe administrateurs.
  - Stockage sécurisé des mots de passe dans un coffre-fort numérique.
2. **Gestion des habilitations :**
  - Profils d'habilitation définis à la remise d'un équipement informatique.
  - Règle de gestion sur Office 365 via Tenant Microsoft Cloud.
  - Suppression des permissions d'accès obsolètes.
  - Revue annuelle des habilitations.
3. **Gestion des incidents et des violations de données :**
  - Une Politique Générale de Sécurité des Systèmes d'Information (PGSSI) est formalisée, ainsi qu'une politique de gestion des incidents de sécurité.
  - Formalisation et mise en œuvre d'une Procédure de gestion des violations de données qui prévoit notamment :
    - Les moyens de notification rapide d'une violation aux clients et utilisateurs.
    - La traçabilité des incidents.
4. **Mesures de sauvegarde et continuité d'activité :**
  - Progiciel de gestion et de comptabilité : Sauvegardes réalisées tous les deux mois.
  - Site web : Sauvegarde effectuée avant tout changement.
5. **Sécurisation des postes de travail et lutte contre les logiciels malveillants :**
  - Verrouillage automatique des sessions.
  - Pare-feu activé sur tous les postes.
  - Antivirus régulièrement mis à jour.
  - Installation automatique des mises à jour de sécurité.
  - Stockage des données sur un espace régulièrement sauvegardé.
  - Exécution restreinte des applications.
6. **Sécurisation de l'informatique mobile :**
  - Chiffrement des équipements mobiles.
  - Verrouillage des smartphones (secret, mot de passe, code, etc.).
7. **Sécurisation des serveurs :**
  - Accès aux outils et interfaces d'administrations limités aux seules personnes habilitées.
  - Installation automatique des mises à jour critiques.
8. **Sécurisation des sites web :** Flux d'échange de données sécurisé (TLS).

9. **Encadrement des développements informatiques :**
  - Réalisation de tests complets avant mis en production.
  - Utilisation de données fictives lors des tests.
10. **Mesures de chiffrement :** utilisation de serveurs chiffrés.
11. **Cloisonnement des données :** via Tenant Microsoft Cloud.
12. **Archivage sécurisé :** archivage sécurisé des données via OVH Snapshot.
13. **Gestion de la sous-traitance :** inclusion de Clauses de sous-traitance RGPD dans les contrats.
14. **Encadrement de la maintenance :** interventions des prestataires encadrées par le responsable de la technologie.
15. **Destruction des données :** destruction des données de manière sécurisé (File Schredder, Clean My Mac).

### Mesures de sécurité spécifiques au logiciel et services associés

1. **Gestion des accès et habilitations :**
  - Chaque collaborateur dispose de droits et d'habilitations définis en fonction son poste et de ses activités.
  - Les équipements sont accessibles uniquement aux personnels autorisés, en fonction de leurs habilitations.
  - Les équipements sont configurés afin que chaque utilisateur s'authentifie pour accéder aux systèmes d'information de la société, garantissant un contrôle individuel des accès et une sécurisation des opérations effectuées.
2. **Traçabilité et journalisation des accès :**
  - Le logiciel dispose d'un système de journalisation permettant d'horodater les accès et de tracer les actions effectuées.
  - Traçabilité complète des interventions : logs des accès, activités réalisées, début et fin des opérations.
3. **Hébergement des données en SaaS :**
  - Hébergement sur des serveurs OVH, pour lesquels les mesures de sécurité OVH sont applicables : [RGPD | Sécurité des infrastructures | OVHcloud France](#).
  - Hébergement HDS sur demande : un contrat spécifique est conclu entre le client et OVH pour l'installation sur un serveur certifié HDS.
4. **Sauvegarde et continuité d'activité :**
  - Sauvegardes régulières :
    - Sauvegardes incrémentales quotidiennes (enregistrement des modifications).
    - Sauvegardes complètes hebdomadaires et à chaque mise à jour du logiciel (minimum 6 par mois).
  - Les sauvegardes sont effectuées sur des serveurs distincts et chiffrés.
  - Tests réguliers de restauration pour garantir l'intégrité des sauvegardes.
  - Ont été formalisés et sont mis en œuvre : un Plan de Reprise d'Activité (PRA), un plan de sauvegarde et un processus de redémarrage d'activité. Ces plans sont testés régulièrement via la mise en œuvre du système de rolling release.
  - Le cas échéant, des Service-level agreement (SLA) sont établis et précisent les délais d'activation du PRA (24 à 48h).

## 5. Mise à jour et maintenance du logiciel :

- Licence On Premise : Les interventions sont réalisées sur demande et autorisation explicite des clients, selon leurs habilitations et systèmes d'authentification.
- Licence SaaS : Système de rolling release qui permet des mises à jour mensuelles ou hebdomadaires pour maintenir la sécurité et les fonctionnalités.

## 6. Mesures de sécurité des serveurs et données :

Mesures mises en œuvre par OVH pour le contrôle et la traçabilité des accès, ainsi que le chiffrement des sauvegardes ; et :

- **Contrôle d'accès** :
  - Accès limité aux serveurs par des personnes habilitées uniquement.
  - Chaque collaborateur dispose d'habilitations définies en fonction de son poste.
- **Chiffrement des données** :
  - Serveurs chiffrés (instances Microsoft).
  - Mots de passe stockés sous forme de hachage sécurisé (hashing).
- **Séparation des serveurs** :
  - Les serveurs de sauvegarde sont distincts des serveurs d'hébergement des données.

## 7. Mesures spécifiques aux logiciels SaaS :

- **Contrôle des accès aux installations** :
  - Chaque membre de l'équipe utilise un ordinateur portable personnel, sécurisé par des codes et authentification individuels.
  - OVH met en œuvre des mesures spécifiques relatives à la gestion des accès aux infrastructures ([RGPD | Sécurité des infrastructures | OVHcloud France](#)).
- **Contrôle des supports de données** :
  - Les supports de données sont protégés contre toute copie, modification ou suppression non autorisée (mesures OVH).

## 8. Gestion des opérations de sous-traitance :

- Les opérations de sous-traitance sont réalisées uniquement par du personnel habilité de Zenlocassur et OVH.
- Politique de gestion des accès à destination du personnel dans le cadre des activités sous-traitées par le client :
  - Accès temporaire et contrôlé aux données (créneaux limités).
  - Traçabilité complète des actions effectuées.
  - Séparation stricte des privilèges d'accès pour limiter les risques.

## 9. Autres mesures :

- Le logiciel intègre les principes de Privacy by Design.
- Effacement physique des données et métadonnées sans délai pour les espaces de stockage courants et les copies répliquées.
- Tests d'intrusion réalisés en mode "boîte noire" (interne et externe).
- Éloignement des sources de risques et protection contre les sources de risques non humaines.