epsight

Version 2026-1

ANNEXE AUX CONDITIONS GÉNÉRALES

# Accord de sous-traitance des données à caractère personnel (RGPD)

| CE DOCUMENT | DOCUMENT ASSOCIÉ | DOCUMENT ASSOCIÉ |
|---|---|---|
| **Accord de sous-traitance RGPD** | **Conditions générales de vente** | **Annexe Data Act** |

Le présent accord est une annexe aux conditions générales d'Epsight (article XIX.II).

## Article I - Objet

Le présent accord (l'« Accord ») définit les conditions dans lesquelles Epsight traite des données à caractère personnel pour le compte du Client dans le cadre des Prestations, conformément à l'article 28 du règlement (UE) 2016/679 du 27 avril 2016 (« RGPD ») et à la loi n° 78-17 du 6 janvier 1978 modifiée.

L'Accord fait partie intégrante du Contrat. En cas de contradiction entre l'Accord et les autres documents contractuels sur la protection des données à caractère personnel, l'Accord prévaut.

## Article II - Définitions

Les termes « données à caractère personnel », « traitement », « responsable du traitement », « sous-traitant », « personne concernée », « violation de données à caractère personnel » et « autorité de contrôle » ont le sens qui leur est donné par l'article 4 du RGPD. Les autres termes commençant par une majuscule ont le sens qui leur est donné par les conditions générales d'Epsight.

**Sous-traitant ultérieur** : désigne tout tiers auquel Epsight confie tout ou partie d'un traitement de Données du Client.

**Données du Client** : désigne les données à caractère personnel traitées par Epsight pour le compte du Client au titre des Prestations.

## Article III - Rôles des Parties

Pour les traitements décrits à l'Annexe 1, le Client agit en qualité de responsable du traitement et Epsight en qualité de sous-traitant. Lorsque le Client agit lui-même en qualité de sous-traitant pour le compte d'un tiers, Epsight intervient en qualité de sous-traitant ultérieur et le Client garantit disposer des autorisations nécessaires.

Epsight agit en qualité de responsable du traitement pour ses propres traitements, notamment la gestion de la relation commerciale, la facturation et la gestion des comptes d'accès à ses outils. Ces traitements ne relèvent pas de l'Accord.

Le Client est seul responsable de la licéité des traitements qu'il confie à Epsight, de l'information des personnes concernées et de la base légale de ces traitements.

## Article IV - Description des traitements

L'objet, la durée, la nature et la finalité des traitements, les catégories de données traitées et les catégories de personnes concernées sont décrits à l'Annexe 1 pour chaque type de Prestation. L'Offre peut les compléter ou les préciser.

Sauf stipulation contraire de l'Offre, Epsight n'accède au contenu des Données du Client que dans la mesure nécessaire à l'exécution des Prestations, notamment pour le support, la supervision, la sauvegarde et la restauration.

## Article V - Instructions du Client

Epsight traite les Données du Client uniquement sur instruction documentée du Client. Le Contrat, l'Offre, l'Accord et les demandes formulées par le Client via le portail client ou l'outil de tickets d'Epsight constituent ces instructions.

Si Epsight considère qu'une instruction constitue une violation du RGPD ou d'une autre disposition relative à la protection des données, elle en informe immédiatement le Client et peut suspendre l'exécution de l'instruction concernée jusqu'à sa confirmation ou sa modification par le Client.

Lorsque Epsight est tenue de procéder à un traitement en vertu du droit de l'Union européenne ou du droit français, elle en informe le Client avant le traitement, sauf si ce droit l'interdit.

## Article VI - Confidentialité

Epsight veille à ce que les personnes autorisées à traiter les Données du Client s'engagent à en respecter la confidentialité ou soient soumises à une obligation légale de confidentialité, et soient informées de leurs obligations en matière de protection des données. L'accès aux Données du Client est limité aux seules personnes qui en ont besoin pour l'exécution des Prestations.

## Article VII - Sécurité

Epsight met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD. Ces mesures sont décrites à l'Annexe 2. Epsight peut les faire évoluer, à condition de ne pas réduire le niveau global de sécurité.

Le Client reste responsable de la sécurité des éléments qu'il administre lui-même, notamment ses postes de travail, ses comptes et mots de passe, ses applications et les configurations qu'il modifie, ainsi que des mesures qui lui incombent au titre de l'Offre.

## Article VIII - Sous-traitants ultérieurs

Le Client donne à Epsight une autorisation générale de recourir aux sous-traitants ultérieurs figurant sur la liste publiée et tenue à jour par Epsight à l'adresse www.epsight.fr/sous-traitants (la « Liste des sous-traitants ultérieurs »), dont les catégories sont décrites à l'Annexe 3.

Epsight informe le Client par e-mail de tout ajout ou remplacement envisagé d'un sous-traitant ultérieur au moins trente (30) jours avant sa prise d'effet. Le Client peut s'y opposer pour un motif légitime lié à la protection des données, par écrit et dans ce délai. Les Parties recherchent alors de bonne foi une solution ; à défaut, le Client peut résilier sans indemnité le Service récurrent concerné par le changement.

Epsight impose à chaque sous-traitant ultérieur, par contrat, des obligations de protection des données au moins équivalentes à celles de l'Accord. Epsight demeure responsable envers le Client de l'exécution de ces obligations par ses sous-traitants ultérieurs.

**Outils d'intelligence artificielle.** Epsight peut utiliser des outils d'intelligence artificielle générative pour l'exécution des Prestations, notamment pour l'analyse d'incidents, la rédaction de documentation ou l'assistance au support. Elle n'y recourt, pour des Données du Client, que dans les conditions suivantes : offre professionnelle de l'éditeur couverte par un accord de sous-traitance conforme à l'article 28 du RGPD ; interdiction contractuelle pour l'éditeur d'utiliser ces données pour entraîner ses modèles ; minimisation, pseudonymisation ou anonymisation des données transmises lorsque c'est possible ; aucun usage de comptes grand public. Les éditeurs concernés figurent sur la Liste des sous-traitants ultérieurs. Le Client peut demander par écrit que ses données ne soient traitées par aucun outil d'intelligence artificielle hébergé hors de l'Espace économique européen ; Epsight l'informe alors des éventuelles conséquences sur les délais ou les modalités d'exécution.

## Article IX - Localisation et transferts

Sauf stipulation contraire de l'Offre, les Données du Client hébergées sur les infrastructures d'Epsight sont stockées dans des centres de données situés en France.

Epsight ne transfère de Données du Client vers un pays situé hors de l'Espace économique européen que vers les sous-traitants ultérieurs figurant sur la Liste des sous-traitants ultérieurs, dans les conditions de l'article VIII, avec l'accord préalable du Client, ou lorsque ce transfert résulte d'un service tiers choisi par le Client (par exemple une Licence d'un éditeur dont les conditions prévoient un tel transfert). Tout transfert est encadré par l'un des mécanismes prévus aux articles 45 à 49 du RGPD, notamment une décision d'adéquation ou les clauses contractuelles types de la Commission européenne.

## Article X - Assistance au Client

Epsight assiste le Client, dans la mesure du possible et compte tenu de la nature du traitement :

- pour répondre aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, limitation, portabilité, opposition). Lorsqu'une personne concernée s'adresse directement à Epsight, celle-ci transmet la demande au Client sans délai et n'y répond pas elle-même, sauf instruction du Client ;
- pour garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, notamment la sécurité, la notification des violations, les analyses d'impact et la consultation préalable de l'autorité de contrôle.

Epsight met à la disposition du Client les informations nécessaires pour démontrer le respect de ses obligations. Elle tient le registre des catégories d'activités de traitement prévu à l'article 30.2 du RGPD. L'assistance qui dépasse la fourniture de ces informations est facturée au tarif en vigueur, sauf si elle résulte d'un manquement d'Epsight.

## Article XI - Violations de données

Epsight notifie au Client toute violation de données à caractère personnel affectant les Données du Client dans les meilleurs délais et au plus tard quarante-huit (48) heures après en avoir pris connaissance, à l'adresse de contact désignée par le Client.

La notification précise, dans la mesure où ces informations sont disponibles : la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables, les mesures prises ou envisagées pour y remédier et le contact chez Epsight. Les informations non disponibles immédiatement sont communiquées de manière échelonnée.

Il appartient au Client, en sa qualité de responsable du traitement, de notifier la violation à l'autorité de contrôle et, le cas échéant, aux personnes concernées. Epsight ne procède à aucune communication publique sur une violation affectant les Données du Client sans l'accord du Client, sauf obligation légale.

## Article XII - Audits

Le Client peut vérifier le respect de l'Accord par Epsight. Il exerce ce droit en priorité sur la base de la documentation, des rapports et des réponses aux questionnaires qu'Epsight met à sa disposition.

Si ces éléments sont insuffisants, le Client peut faire réaliser un audit sur pièces ou sur place, au plus une fois par an sauf violation de données ou demande d'une autorité de contrôle, moyennant un préavis de trente (30) jours. L'audit est réalisé par le Client ou par un auditeur indépendant qui n'est pas un concurrent d'Epsight et qui est tenu à la confidentialité. Il ne peut porter atteinte à la sécurité des infrastructures d'Epsight ni aux données de ses autres clients ; l'accès aux centres de données est soumis aux règles de leurs opérateurs. Les frais de l'audit sont à la charge du Client, ainsi que le temps passé par Epsight au-delà d'une journée, sauf si l'audit révèle un manquement significatif d'Epsight.

## Article XIII - Sort des données en fin de Prestation

A la fin d'une Prestation, et au choix du Client exprimé par écrit, Epsight restitue les Données du Client concernées puis les supprime, ou les supprime directement, dans les conditions prévues à l'article XXIV.IV des conditions générales et, pour les services de traitement de données, dans l'annexe Data Act. Les copies de sauvegarde sont supprimées à l'expiration de leur durée de rétention, telle que définie dans l'Offre ou, à défaut, dans la politique de sauvegarde applicable au Client.

Epsight peut conserver les Données du Client lorsque le droit de l'Union européenne ou le droit français l'exige, en les protégeant dans les conditions de l'Accord. Sur demande, Epsight atteste par écrit de la suppression.

## Article XIV - Responsabilité

Chaque Partie est responsable des manquements à ses obligations au titre du RGPD et de l'Accord. La responsabilité d'Epsight au titre de l'Accord est soumise aux limitations de l'article XX des conditions générales, sauf disposition légale contraire. Les amendes administratives prononcées contre une Partie restent à sa charge.

## Article XV - Durée

L'Accord prend effet à la signature de la première Offre qui y renvoie. Il reste en vigueur tant qu'Epsight traite des Données du Client, y compris après la fin du Contrat jusqu'à la restitution ou la suppression complète des Données du Client.

Epsight peut faire évoluer l'Accord pour tenir compte d'une évolution de la réglementation, d'une recommandation de l'autorité de contrôle ou de ses services, dans les conditions de l'article I des conditions générales, sans pouvoir réduire le niveau de protection des Données du Client.

**Contact protection des données Epsight** : dpo@epsight.fr.

## Annexe 1 - Description des traitements

La nature des Données du Client dépend de ce que le Client stocke ou fait circuler sur les systèmes confiés à Epsight : Epsight n'en détermine ni le contenu ni la finalité. La durée de chaque traitement est celle de la Prestation concernée, prolongée de la période de restitution et de suppression de l'article XIII.

| Prestation | Nature des opérations | Finalité | Catégories de données | Personnes concernées |
|---|---|---|---|---|
| **Hébergement sur plateforme mutualisée, location de serveurs dédiés** | Stockage, hébergement, réplication entre centres de données, accès technique pour l'administration | Fournir l'infrastructure sur laquelle le Client exécute ses systèmes | Toutes données présentes dans les machines et volumes du Client, potentiellement y compris des données sensibles selon l'activité du Client | Salariés, clients, fournisseurs, usagers et tout tiers dont le Client traite les données |
| **Housing (hébergement d'équipements du Client)** | Aucun accès logique aux données, sauf intervention demandée par le Client | Accueillir les équipements du Client et leur fournir énergie et connectivité | Données stockées sur les équipements du Client, lors des seules interventions | Idem |
| **Sauvegarde externalisée** | Copie, stockage, chiffrement, restauration, suppression à expiration | Permettre la restauration des systèmes et données du Client | Toutes données incluses dans le périmètre des jobs de sauvegarde | Idem |
| **Infogérance, maintien en conditions opérationnelles et de sécurité, maintenance** | Accès, consultation, modification de configurations, gestion des comptes et des droits, mises à jour, diagnostic | Administrer et maintenir les systèmes du Client | Données d'annuaire (identités, identifiants, groupes), journaux techniques, et contenu des systèmes lorsque l'intervention l'exige | Utilisateurs et administrateurs du Client, et personnes dont les données figurent dans les systèmes |
| **Supervision et cybersécurité managée (EDR, XDR, MDR)** | Collecte et analyse d'événements et de journaux, détection, investigation, remédiation | Détecter et traiter les incidents de sécurité et de disponibilité | Journaux de connexion et d'activité, noms d'utilisateurs, adresses IP, noms de machines, fichiers suspects | Utilisateurs des postes et serveurs du Client |
| **Licences et services d'éditeurs** | Création et gestion des comptes et des abonnements | Fournir et administrer les Licences | Nom, adresse e-mail, fonction et identifiants des utilisateurs | Utilisateurs désignés par le Client |
| **Support (tickets, assistance)** | Réception, consultation, échange, conservation | Traiter les demandes du Client | Contenu des demandes, pièces jointes, captures d'écran | Demandeurs et personnes citées dans les demandes |

Le Client informe Epsight par écrit si les systèmes confiés contiennent des données de santé, des données soumises à une réglementation sectorielle ou des données relevant de l'article 9 du RGPD, afin que les mesures appropriées soient définies dans l'Offre. L'hébergement de données de santé au sens de l'article L 1111-8 du Code de la santé publique n'est pas couvert par l'Accord, Epsight n'étant pas certifiée hébergeur de données de santé.

## Annexe 2 - Mesures techniques et organisationnelles

Les mesures ci-dessous s'appliquent aux infrastructures opérées par Epsight. Les mesures propres à une Prestation (chiffrement dédié, rétention spécifique, niveau de service) sont précisées dans l'Offre.

| Domaine | Mesures |
|---|---|
| **Sécurité physique** | Infrastructures hébergées dans deux centres de données tiers situés en France, distants d'environ 30 km, avec contrôle d'accès, vidéosurveillance, alimentation et climatisation redondées, selon les engagements de l'opérateur |
| **Disponibilité et résilience** | Architecture répartie sur les deux centres de données ; stockage distribué et répliqué ; supervision continue des infrastructures. L'élaboration du plan de reprise d'activité du Client relève du Client, qui peut l'appuyer sur l'infrastructure répartie sur deux sites d'Epsight, sauf prestation spécifique prévue dans l'Offre |
| **Contrôle d'accès logique** | Modèle d'administration par niveaux (tiering) séparant les comptes d'administration des infrastructures critiques ; comptes nominatifs ; principe du moindre privilège ; authentification multifacteur pour tous les accès d'administration ; revue semestrielle des droits |
| **Réseau** | Pare-feu de nouvelle génération ; segmentation et cloisonnement des environnements clients ; réseau d'administration hors bande (OOB) séparé des réseaux de production ; accès distants chiffrés |
| **Chiffrement et secrets** | Infrastructure de clés publiques interne avec autorité racine hors ligne et clés protégées par module matériel (HSM) ; chiffrement des flux d'administration ; chiffrement des sauvegardes au repos ; coffre-fort de mots de passe hébergé sur les infrastructures d'Epsight en France, aucun secret n'étant stocké dans les outils de documentation |
| **Sauvegarde** | Sauvegardes régulières selon la politique définie dans l'Offre ; sauvegardes chiffrées ; copies sur un site distinct ; tests de restauration réalisés lors des opérations de maintenance ou à la demande du Client |
| **Détection et réponse** | Protection des terminaux et serveurs par une solution EDR d'un éditeur européen ; journalisation des accès d'administration conservée douze (12) mois ; procédure de gestion des incidents et des violations de données |
| **Gestion des vulnérabilités** | Veille sur les vulnérabilités des produits opérés ; application des correctifs selon leur criticité, avec pour objectif dix (10) jours pour les vulnérabilités critiques et trente (30) jours pour les vulnérabilités importantes, sous réserve de la disponibilité du correctif et des fenêtres de maintenance convenues |
| **Personnel** | Engagement de confidentialité de chaque salarié et intervenant ; accès limité au besoin d'en connaître ; information des intervenants sur leurs obligations de sécurité et de protection des données ; retrait des accès au départ |
| **Postes de travail Epsight** | Postes gérés, chiffrés et protégés par EDR ; travail à distance via des accès sécurisés |
| **Effacement** | Suppression logique des volumes et sauvegardes à la fin des Prestations ; aucun support de stockage ne quitte les infrastructures d'Epsight sans avoir été effacé de manière sécurisée par Epsight ou, lorsque l'effacement n'est pas possible, détruit physiquement |

## Annexe 3 - Sous-traitants ultérieurs

Seuls les outils et prestataires qui traitent des Données du Client sont des sous-traitants ultérieurs. Les outils internes d'Epsight qui n'y ont pas accès (comptabilité, paie, outils de conception sans données clients) n'y figurent pas.

La liste nominative est publiée à l'adresse www.epsight.fr/sous-traitants et tenue à jour dans les conditions de l'article VIII. Elle relève des catégories suivantes :

- hébergement physique des infrastructures ;
- éditeurs de solutions de sécurité (EDR, XDR, MDR, filtrage) ;
- supervision, administration à distance et gestion des terminaux ;
- sauvegarde et stockage externalisés ;
- distribution de Licences ;
- support, tickets et gestion de la relation client ;
- messagerie, collaboration et signature électronique ;
- documentation technique ;
- outils d'intelligence artificielle ;
- intervenants indépendants.

Liste en vigueur à la date du présent Accord :

| Sous-traitant | Service rendu | Données concernées | Localisation | Encadrement des transferts |
|---|---|---|---|---|
| **Etix Everywhere** | Hébergement physique des infrastructures dans deux centres de données à Nantes | Aucun accès logique ; hébergement des supports physiques | France | Sans objet |
| **Bitdefender SRL** | Solution EDR et XDR (console GravityZone hébergée chez OVHcloud) et service MDR opéré par Bitdefender | Journaux et événements de sécurité, fichiers suspects | France (OVHcloud) ; centre opérationnel de sécurité du service MDR en Roumanie (Union européenne) | Sans objet (Union européenne) |
| **Distributeurs de licences : Arrow ECS France, Ingram Micro, TD Synnex, Exclusive Networks, Itancia, Also** | Commande et gestion des Licences auprès des éditeurs (Epsight revendeur de niveau 2) | Nom, adresse e-mail et identifiants des utilisateurs, informations du compte ou du locataire du Client | France (entités françaises des distributeurs) ; les plateformes de commande de certains distributeurs recourent à des prestataires hors Union européenne, encadrés par l'accord de protection des données de chaque distributeur | Sans objet (Union européenne) |
| **Microsoft Ireland Operations Ltd** | Messagerie, collaboration et stockage documentaire d'Epsight (Exchange, Teams, SharePoint, OneDrive) et assistant Microsoft 365 Copilot | Échanges avec le Client, pièces jointes, documents et documentation technique relatifs aux environnements clients | Union européenne (EU Data Boundary) ; États-Unis pour les fonctions de Copilot utilisant les modèles d'Anthropic, sous-traitant de Microsoft couvert par l'accord de protection des données de Microsoft | Clauses contractuelles types et Data Privacy Framework pour les accès résiduels |
| **Atlassian Pty Ltd (Australie)** | Documentation technique des environnements clients (Confluence) | Données d'architecture et de configuration, noms de comptes | Union européenne (résidence des données configurée) ; certaines données de compte et métadonnées peuvent rester traitées hors UE | Clauses contractuelles types intégrées à l'accord de sous-traitance d'Atlassian et Data Privacy Framework pour les flux résiduels ; utilisation des données pour l'entraînement des modèles désactivée |
| **Zoho Corporation B.V. (Pays-Bas)** | Signature électronique (Zoho Sign) | Noms, adresses e-mail des signataires, documents signés (devis, contrats) | Union européenne (centre de données européen de Zoho) ; accès ponctuels du support depuis l'Inde | Clauses contractuelles types entre les entités néerlandaise et indienne de Zoho pour les accès du support |
| **Anthropic Ireland, Limited** | Assistant d'intelligence artificielle (Claude Team) | Extraits de journaux, de configurations, de tickets et de documents transmis pour analyse, minimisés autant que possible | États-Unis | Clauses contractuelles types intégrées à l'accord de sous-traitance de l'éditeur |
| **Intervenants indépendants d'Epsight** | Renfort technique sur les Prestations | Accès aux systèmes du Client dans le cadre de leurs interventions | France | Sans objet ; engagement de confidentialité et conditions identiques à l'Accord |

Les sous-traitants ultérieurs propres à une Licence (par exemple l'éditeur d'un service en ligne) relèvent des conditions de cet éditeur, que le Client accepte en souscrivant la Licence.