

Accord sur le traitement des données

Version 1.1 – août 2026

Le présent accord sur le traitement des données (« **ATD** ») est conclu entre :

- 2) **Le Client**, agissant en tant que **Responsable du traitement** ; et
- 2) **Secutec BV**, société constituée en vertu du droit belge, dont le siège social est situé Boomsesteenweg 41/11, 2630 Aartselaar, Belgique, numéro d'entreprise 0875.719.463 (« Secutec »), agissant en tant que **sous-traitant**.

Le Client et Secutec sont chacun une « **Partie** » et ensemble les « **Parties** ».

Le présent ATD fait partie intégrante de l'accord entre les parties et régit le traitement des données à caractère personnel par Secutec pour le compte du client.

1 Définitions

Tous les termes en majuscules non définis dans le présent document ont la signification qui leur est donnée dans le Contrat.

- « **Affilié** » désigne toute entité contrôlant, contrôlée par ou sous contrôle commun avec une Partie.
- « **Contrat** » désigne le contrat conclu entre le Client et Secutec pour la fourniture des produits et services de Secutec.
- « **Données à caractère personnel du client** » désigne les données à caractère personnel traitées par Secutec en tant que sous-traitant pour le compte du client dans le cadre de l'accord.
- « **Lois sur la protection des données** » désigne le RGPD et toutes les législations belges et européennes applicables qui le complètent ou le mettent en œuvre.
- « **Demande de la personne concernée** » désigne une demande émanant d'une personne concernée visant à exercer ses droits en vertu du RGPD.
- « **Sous-traitant ultérieur** » désigne tout tiers engagé par Secutec pour traiter les données à caractère personnel du client.
- Les termes tels que « **Responsable du traitement** », « **Sous-traitant** », « **Traitement** », « **Données à caractère personnel** », « **Violation de données à caractère personnel** », « **Autorité de contrôle** », etc. ont la signification qui leur est donnée dans le RGPD.

2 Champ d'application du ATD

Le présent ATD s'applique à tous les traitements effectués par Secutec dans le cadre des services utilisés par le client. Les activités de traitement qui s'appliquent à tous les clients, quels que soient les services qu'ils achètent, sont décrites dans ***l'annexe A – Plateforme SecureSIGHT et application mobile***.

En cas de conflit entre le présent ATD et tout autre document contractuel, le présent ATD prévaut en matière de protection des données. Le présent ATD régit uniquement le traitement des données à caractère personnel du client. Le traitement de données anonymisées ou agrégées qui ne se rapportent plus à une personne identifiable n'entre pas dans le champ d'application du présent ATD.

3 Rôles des parties

Le client agit en tant que responsable du traitement et détermine les finalités et les moyens du traitement des données personnelles du client dans le cadre du contrat.

Secutec agit en tant que sous-traitant et traite les données personnelles du client uniquement sur la base d'instructions documentées du client, sauf si la loi applicable exige qu'il en soit autrement.

Lorsque Secutec traite des données agrégées et/ou anonymisées qui ne peuvent raisonnablement être réidentifiées, compte tenu des moyens disponibles, du coût, du temps et de la technologie, Secutec agit en tant que responsable indépendant du traitement des données à des fins telles que la veille sur les menaces, l'analyse statistique, l'optimisation des services, la recherche en matière de sécurité et l'analyse des plateformes.

Ce traitement est régi par la propre politique de confidentialité de Secutec et n'implique pas les données personnelles du client au sens du présent ATD.

4 Instructions documentées

Secutec traitera les données personnelles du client en stricte conformité avec les instructions documentées du client, sauf si la législation de l'UE ou d'un État membre en dispose autrement.

Si Secutec estime qu'une instruction enfreint les lois sur la protection des données, Secutec en informera le client et pourra suspendre le traitement concerné.

Secutec n'est pas tenue d'évaluer si l'utilisation des services par le client est conforme aux lois sur la protection des données.

5 Confidentialité

Secutec veillera à ce que toutes les personnes autorisées à traiter les données personnelles du client soient soumises à des obligations de confidentialité appropriées, qu'elles soient contractuelles ou légales.

6 Mesures de sécurité

Secutec mettra en œuvre et maintiendra les mesures de sécurité techniques et organisationnelles décrites à ***l'annexe B - Mesures de sécurité techniques et organisationnelles***, qui s'appliquent à tous les traitements effectués dans le cadre du présent ATD.

Le Client reconnaît que ces mesures offrent un niveau de sécurité adapté au risque, compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature du Traitement (art. 32 du RGPD).

7 Sous-traitance

7.1 Autorisation générale

Le Client accorde à Secutec une autorisation générale pour engager des Sous-traitants auxiliaires pour le Traitement des Données personnelles du Client dans le cadre des Services.

L'annexe C - Sous-traitants décrit, à un niveau catégorique, les types de sous-traitants pouvant être engagés par Secutec, sans énumérer les fournisseurs individuels, reflétant ainsi la nature indépendante des fournisseurs et évolutive des technologies de cybersécurité. À des

fins de transparence, Secutec tient à jour une liste indicative des sous-traitants décrivant des exemples de sous-traitants actuellement utilisés dans la prestation de ses services.

Cette liste est fournie à titre informatif uniquement et ne fait pas partie du présent accord sur le traitement des données. La liste des sous-traitants peut être mise à jour de temps à autre afin de refléter l'évolution technologique, les changements d'infrastructure ou les améliorations apportées aux services.

Les sous-traitants sont engagés et régis conformément aux principes énoncés dans le présent article 7 et à l'annexe C (Sous-traitants).

Secutec peut nommer, remplacer ou révoquer des sous-traitants en sous-traitance selon les besoins pour fournir les services, maintenir la sécurité, assurer la continuité du service ou se conformer aux exigences légales ou réglementaires applicables.

7.2 Notification et objection

Secutec mettra à la disposition du client des informations concernant les modifications apportées aux catégories de sous-traitants engagés pour le traitement des données personnelles du client.

Le Client peut s'opposer à ces modifications pour des motifs raisonnables et documentés liés à la protection des données, en tenant compte de la nature des Services et du rôle des Sous-traitants dans les opérations de sécurité de Secutec.

En cas d'objection, les Parties discuteront de la question de bonne foi. Si aucune alternative raisonnable ne peut être convenue, le Client peut résilier uniquement la partie concernée des Services, sans droit à des dommages-intérêts, indemnités ou pénalités liés à cette résiliation.

Les modifications nécessaires pour des raisons de sécurité, de réponse aux incidents, de continuité du service ou de conformité peuvent être mises en œuvre immédiatement. Dans ce cas, Secutec en informera le client sans délai injustifié.

7.3 Obligations et responsabilité des sous-traitants

Secutec veillera à ce que tout sous-traitant engagé soit soumis à des obligations en matière de protection des données qui ne soient pas moins protectrices que celles énoncées dans le présent ATD, y compris des mesures de sécurité techniques et organisationnelles appropriées. Secutec reste entièrement responsable de la performance de ses sous-traitants conformément au présent ATD, dans la même mesure que si le traitement était effectué directement par Secutec.

Secutec reste pleinement responsable des actions et omissions de ses sous-traitants dans la même mesure que si elle effectuait elle-même le traitement.

8 Transferts internationaux de données

Les données à caractère personnel relatives au trafic provenant de l'UE sont principalement traitées au sein de l'Union européenne.

Lorsque le traitement en dehors de l'Espace économique européen est nécessaire pour la fourniture des services, ces transferts sont effectués conformément aux lois applicables en matière de protection des données et sous réserve de garanties appropriées, y compris des clauses contractuelles types ou d'autres mécanismes de transfert valables.

9 Assistance au client

Secutec assistera le client, dans la mesure du possible, pour :

- répondre aux demandes des personnes concernées ; Secutec ne répondra directement à aucune demande d'une personne concernée, sauf instruction expresse du client.
- se conformer aux articles 32 à 36 du RGPD (sécurité, notification des violations, AIPD, consultation préalable).

Secutec peut facturer des frais raisonnables lorsque l'assistance dépasse les niveaux de service normaux, à condition d'en informer le client à l'avance.

Cette assistance n'inclut pas la réalisation d'évaluations juridiques, le respect des obligations légales du client ou la mise en œuvre de mesures organisationnelles dans l'environnement du client.

10 Droits d'audit

Le client peut effectuer des audits afin de vérifier la conformité de Secutec au présent ATD, sous réserve :

- un préavis écrit de 60 jours ;
- un maximum d'un audit tous les 12 mois ;
- les audits soient effectués pendant les heures normales de bureau ;
- l'interdiction d'accéder aux informations financières internes de Secutec, aux données d'autres clients, aux rapports d'audit interne ou aux secrets commerciaux ;

À titre alternatif, Secutec peut satisfaire à ses obligations d'audit en fournissant des certificats ISO 27001 récents ou des résumés d'audits ISO 27001 externes.

Le client doit s'assurer que tout audit ne perturbe pas de manière déraisonnable les activités commerciales de Secutec et n'implique pas des auditeurs qui sont des concurrents directs de Secutec.

11 Notification de violation des données à caractère personnel

Secutec informera le client sans délai dès qu'elle aura connaissance d'une violation des données à caractère personnel affectant les données à caractère personnel du client.

La notification doit inclure la nature de la violation, les catégories de données concernées, les conséquences probables et les mesures prises ou proposées pour remédier à la violation.

Le client reste responsable de toute notification aux autorités de contrôle et aux personnes concernées, sauf accord contraire. Le client doit informer Secutec sans délai dès qu'il a connaissance d'un incident de sécurité qui :

- affecte les données à caractère personnel pour lesquelles Secutec agit en tant que sous-traitant ; ou
- affecte toute information confidentielle, tout identifiant, tout jeton d'accès, tout fichier de preuve, tout rapport ou toute autre donnée fournie par Secutec au client.

Cette notification doit inclure, dans la mesure où cela est connu, une description de la nature de l'incident et de son impact potentiel sur les données ou les systèmes de Secutec.

Aucune disposition de la présente clause n'oblige le client à informer Secutec des violations de données à caractère personnel pour lesquelles le client est le responsable du traitement, sauf si les données ou les systèmes de Secutec sont affectés.

12 Restitution et suppression des données à caractère personnel

À la résiliation du Contrat, les Données personnelles du Client ne seront conservées que pendant la durée nécessaire, conformément aux principes de conservation et aux périodes de conservation applicables définis à l'Annexe D – Principes de conservation, sauf si une période de conservation plus longue est requise par la loi applicable ou convenue par écrit.

À l'expiration des périodes de conservation applicables, Secutec supprimera ou anonymisera les données personnelles du client dans un délai raisonnable, à l'exception des sauvegardes cryptées qui sont écrasées conformément au calendrier standard de rotation des sauvegardes de Secutec.

Le client peut demander la restitution des données personnelles avant leur suppression.

13 Responsabilité

Les dispositions du Contrat en matière de responsabilité s'appliquent également au présent ATD.

Aucune disposition du présent ATD ne limite les droits des personnes concernées en vertu de l'article 82 du RGPD.

14 Loi applicable et juridiction compétente

Le présent ATD est régi par le droit belge.

Tout litige sera soumis à la compétence exclusive des tribunaux d'Anvers.

15 Hiérarchie

En cas d'incohérence :

1. Le présent ATD prévaut sur le Contrat ;
2. Les annexes prévalent sur le présent ATD dans la mesure où elles décrivent le traitement spécifique au service.

À tous autres égards, les dispositions du présent ATD prévalent sur toute disposition contradictoire figurant dans une annexe.

Pour éviter toute ambiguïté, les annexes décrivant les activités de traitement, les sous-traitants ou les principes de conservation doivent être interprétées conformément aux dispositions applicables du présent ATD et sous réserve de celles-ci.

Le présent ATD restera en vigueur tant que Secutec traitera les données à caractère personnel du client dans le cadre de l'accord.

16 Structure des annexes

Les annexes suivantes font partie intégrante et indissociable du présent accord sur le traitement des données :

Annexe A – Plateforme SecureSIGHT et application mobile

Décrit les activités de traitement inhérentes à la plateforme SecureSIGHT et à l'application mobile, qui s'appliquent à tous les clients, quels que soient les services qu'ils achètent.

Annexe B – Mesures de sécurité techniques et organisationnelles (TOM)

Définit les contrôles de sécurité de Secutec conformes à la norme ISO 27001 applicables à tous les traitements effectués dans le cadre du présent accord sur le traitement des données.

Annexe C – Sous-traitants

Décrit, à un niveau catégorique, les types de sous-traitants susceptibles d'être engagés par Secutec dans le cadre de la fourniture des services, conformément au modèle d'autorisation générale défini à l'article 7.

Annexe D – Principes de conservation

Décrit les périodes de conservation par défaut pour le traitement des données personnelles des clients dans tous les services.

Annexe A – Plateforme SecureSIGHT et application mobile

Cette annexe décrit le traitement des données à caractère personnel effectué via la plateforme web SecureSIGHT et l'application mobile MySecutec (collectivement, « **la plateforme** »).

La Plateforme fournit des services d'authentification, de gestion des utilisateurs, des tableaux de bord, des alertes et l'accès aux Services de Secutec.

La présente annexe s'applique à tous les clients, quels que soient les services qu'ils achètent, car tous les clients utilisent la plateforme pour accéder à leur compte et le gérer.

Les termes non définis ici ont la signification qui leur est donnée dans l'ADP.

1 Champ d'application du traitement

La Plateforme sert de couche d'accès unifiée pour tous les modules Secutec.

La plateforme traite les données relatives aux utilisateurs, à l'authentification, les données techniques et les données d'accès, tandis que les modules sous-jacents traitent les données opérationnelles de cybersécurité.

La Plateforme ne prend pas de décisions indépendantes concernant les données opérationnelles de sécurité ; elle se contente de les afficher.

Secutec traite uniquement le minimum de données personnelles et techniques nécessaires pour fournir l'accès et les fonctionnalités de la plateforme, y compris les données d'authentification, les journaux d'accès et les métadonnées opérationnelles, strictement limitées à la fourniture de services, à l'assistance, à la sécurité et à l'auditabilité.

2 Rôles des parties

2.1 Rôle du sous-traitant

Secutec agit en tant que sous-traitant pour les données personnelles nécessaires pour fournir aux clients l'accès et les fonctionnalités de la plateforme, notamment :

- Comptes utilisateurs
- Authentification et contrôle d'accès
- Journalisation et métadonnées de session
- Accès au tableau de bord
- Chat d'assistance

2.2 Rôle du contrôleur

Pour l'analyse, le diagnostic des pannes et la surveillance des performances au sein de la plateforme,

Secutec agit en tant que responsable du traitement indépendant.

Ce traitement est effectué dans le but de :

- améliorer la stabilité et les performances
- dépanner les erreurs ou les plantages
- assurer la qualité du service

Ce traitement par le responsable du traitement n'implique pas les données opérationnelles du client.

Pour ce traitement, la politique de confidentialité de Secutec s'applique.

3 Catégories de données à caractère personnel

La plateforme traite les catégories suivantes de données à caractère personnel :

3.1 Données du compte utilisateur

- Nom complet
- Adresse e-mail
- Organisation / locataire
- Rôles et autorisations de l'utilisateur
- Modules liés et configuration des services

3.2 Données d'authentification et de sécurité

- E-mail + mot de passe haché
- Données de vérification MFA/OTP
- Horodatage d'authentification
- Identifiants de session
- Journaux des tentatives de connexion
- Adresse IP lors de la connexion

3.3 Données techniques et relatives à l'appareil

- Type d'appareil, version du système d'exploitation, modèle de l'appareil
- Version de l'application
- Métadonnées du navigateur ou de l'application
- Indicateurs de performance
- Métadonnées de diagnostic des plantages
- Aucune donnée de géolocalisation n'est collectée.

3.4 Données de notification push

La plateforme peut envoyer des notifications push. Pour cela, des jetons de notification sont traités.

3.5 Données d'utilisation

- Affichages d'écran
- Événements de navigation
- Utilisation des fonctionnalités

- Durée de session

3.6 Données d'assistance et de communication

- Messages de chat dans l'application
- horodatages et identifiants de l'expéditeur

3.7 Finalités du traitement

Les données personnelles sont traitées via la plateforme aux fins suivantes :

1. Authentification des utilisateurs et accès sécurisé
2. Contrôle d'accès basé sur les rôles
3. Affichage des tableaux de bord des services et des informations opérationnelles
4. Assistance et communication
5. Maintien de la sécurité, de la journalisation et de l'auditabilité
6. Surveillance des performances et détection des erreurs (rôle de contrôleur)

Aucune donnée à caractère personnel n'est utilisée à des fins de marketing ou de profilage sans rapport avec le service.

4 Sous-traitants

Les activités de traitement visées dans la présente annexe peuvent impliquer le recours à des sous-traitants, comme décrit de manière catégorique dans l'annexe C (Sous-traitants).

L'annexe C identifie les types et catégories de sous-traitants susceptibles d'être engagés par Secutec dans le cadre des services, sans énumérer les fournisseurs individuels.

Les sous-traitants peuvent être engagés, remplacés ou mis à jour conformément à l'article 7 de l'accord de traitement des données, en tenant compte de la nature indépendante des fournisseurs et évolutive des technologies de cybersécurité.

5 Périodes de conservation

Toutes les périodes de conservation applicables aux données à caractère personnel traitées en vertu de la présente annexe sont régies exclusivement par l'annexe D (Principes de conservation).

La présente annexe décrit les catégories de données à caractère personnel traitées par la Plateforme, mais ne définit ni ne modifie les durées de conservation.

L'annexe D constitue la seule source fiable pour les périodes de conservation applicables aux données à caractère personnel liées à la Plateforme.

6 Mesures de sécurité

Tout traitement effectué en vertu de la présente annexe est protégé par les mesures techniques et organisationnelles décrites à l'**annexe B (Mesures de sécurité)**.

Celles-ci comprennent :

- MFA
- Chiffrement en transit et au repos
- Hébergement sécurisé et isolation des locataires
- Journalisation et détection des anomalies

- RBAC
- Gestion des vulnérabilités

7 Responsabilités du client

Le client doit:

- s'assurer que ses utilisateurs autorisés conservent des identifiants sécurisés
- gérer les droits d'accès et les rôles
- veiller à la surveillance légale des comptes des employés associés à la plateforme
- éviter de stocker des données personnelles inutiles ou excessives dans les canaux d'assistance
- veiller à l'utilisation sécurisée des appareils qui accèdent à la Plateforme

8 Remarques supplémentaires

- La plateforme est strictement réservée au commerce interentreprises (B2B) et n'est pas destinée à être utilisée par les consommateurs.
- L'application est une interface complémentaire ; elle ne remplace pas la plateforme web SecureSIGHT complète.
- Les fonctionnalités d'usurpation d'identité sont réservées aux partenaires autorisés.

Annexe B – Mesures de sécurité techniques et organisationnelles

Secutec met en œuvre les mesures techniques et organisationnelles suivantes (« TOM ») afin de garantir un niveau de sécurité adapté au risque associé au traitement des données à caractère personnel des clients, conformément à l'article 32 du RGPD.

Ces mesures s'appliquent à tous les services, sauf si des mesures supplémentaires sont ajoutées dans des annexes supplémentaires.

1 Système de gestion de la sécurité de l'information (SGSI)

1.1 Cadre ISO 27001

Secutec maintient un système de gestion de la sécurité de l'information (SGSI) formel conforme à la norme ISO/IEC 27001.

L'ISMS régit l'approche de Secutec en matière de confidentialité, d'intégrité et de disponibilité des actifs informationnels.

1.2 Politiques documentées

Le SGSI s'appuie sur un ensemble complet de politiques documentées, comprenant notamment (liste non exhaustive) :

- Politique de sécurité de l'information
- Politique de contrôle d'accès
- Politique de sécurité du réseau
- Politique de sécurité des opérations
- Politique de cryptographie et de gestion des clés
- Politique de sécurité des ressources humaines
- Politique de gestion des actifs
- Politique de continuité des activités et de reprise après sinistre
- Politique de sécurité physique
- Politique de gestion des fournisseurs et des tiers
- Politique de développement sécurisé et de gestion du changement
- Politique de gestion des incidents
- Politique de conformité
- Politique de gouvernance et d'évaluation des risques du SMSI

Ces politiques internes ne font pas partie du contrat et peuvent être mises à jour de temps à autre dans le cadre de l'amélioration continue prévue par la norme ISO 27001.

1.3 Preuve de conformité

À la demande du client, Secutec peut fournir des preuves de la mise en œuvre du SMSI, telles que :

- certificats ISO/IEC 27001 et déclarations de portée,
- des rapports d'audit sommaires,
- des attestations de conformité.

Les documents relatifs à la politique interne et les détails opérationnels sensibles ne sont pas communiqués dans leur intégralité pour des raisons de sécurité.

2 Mesures de contrôle d'accès

2.1 Principe du moindre privilège

L'accès aux données personnelles des clients est strictement limité au strict nécessaire.

2.2 Authentification et autorisation

Une authentification multifactorielle est requise pour l'accès administratif.

Des identités utilisateur uniques sont imposées.

Les droits d'accès sont révisés périodiquement.

2.3 Révocation immédiate

L'accès est révoqué immédiatement en cas de changement de fonction ou de cessation d'emploi.

3 Sécurité physique et environnementale

Les données personnelles des clients sont principalement hébergées dans des centres de données sécurisés, gérés de manière professionnelle et basés dans l'EEE, appartenant à des fournisseurs de services cloud certifiés.

Lorsque le traitement en dehors de l'EEE est nécessaire, des mesures de protection appropriées sont appliquées conformément à la DPA et aux lois applicables en matière de protection des données.

Les centres de données assurent le contrôle physique des accès, la protection environnementale, la détection des incendies, la redondance et une surveillance 24 heures sur 24, 7 jours sur 7.

4 Encryption et protection des données

Encryption en transit : tous les canaux de communication utilisés pour transférer les données personnelles des clients sont sécurisés à l'aide du protocole TLS 1.2+ ou d'un protocole équivalent.

Encryption au repos : les journaux, les données DNS et les données de service sont chiffrés au repos à l'aide d'algorithmes conformes aux normes de l'industrie.

Les clés cryptographiques sont gérées de manière sécurisée.

5 Sécurité du réseau

Secutec applique la segmentation du réseau, des pare-feu et des systèmes de détection/prévention des intrusions

Le trafic DNS et spécifique aux services est surveillé afin de détecter les anomalies et les activités malveillantes. Des protections anti-DDoS et des mécanismes de limitation du débit protègent la disponibilité des services.

6 Sécurité des opérations

Des pratiques de codage sécurisées et des évaluations par les pairs sont appliquées pour les composants développés en interne.

Tous les systèmes sont soumis à des analyses régulières de vulnérabilité et des correctifs sont appliqués en fonction de leur gravité.

La journalisation des événements liés à la sécurité est gérée de manière centralisée et surveillée. L'accès aux données personnelles des clients est consigné et les journaux sont régulièrement examinés.

Des procédures de sauvegarde garantissent la capacité de restauration des données ; les sauvegardes sont cryptées.

7 Détection et réponse aux incidents

Secutec dispose d'un plan d'intervention en cas d'incident conforme aux normes ISO 27001 et NIS2.

Les incidents de sécurité font l'objet d'une enquête, sont documentés et maîtrisés rapidement.

En cas de violation des données personnelles affectant les données personnelles des clients, Secutec en informera le client sans délai, conformément à l'article 11 du DPA.

8 Continuité des activités et reprise après sinistre

Les services sont principalement déployés sur une infrastructure cloud redondante au sein de l'EEE.

Les procédures de reprise après sinistre sont testées périodiquement.

Les systèmes critiques sont surveillés 24 heures sur 24 et 7 jours sur 7 afin d'en garantir les performances et la disponibilité.

9 Gestion des fournisseurs et des sous-traitants

Les sous-traitants sont évalués sur le plan de la sécurité avant leur intégration.

Seuls les sous-traitants disposant des certifications appropriées (par exemple, ISO 27001) sont engagés.

Les contrats conclus avec les sous-traitants comprennent des obligations équivalentes à celles imposées par l'autorité de protection des données.

10 Minimisation et conservation des données

Secutec ne traitera que la quantité minimale de données à caractère personnel et de données techniques nécessaires à la fourniture des services conformément au présent contrat.

Ces données peuvent inclure les données fournies par le client, les données de sécurité opérationnelle, les données d'authentification et d'accès, les métadonnées d'alerte et les informations accessibles au public, strictement limitées à ce qui est nécessaire pour la prestation de services, les enquêtes, les rapports et les opérations de sécurité.

La conservation de ces données est régie exclusivement par l'annexe D (Principes de conservation).

11 Tests et amélioration continue

Des tests de sécurité sont effectués périodiquement.

Les résultats sont suivis et corrigés en fonction du risque.

Les TOM sont révisées au moins une fois par an et mises à jour si nécessaire.

Annexe C – Sous-traitants

1 Champ d'application

La présente annexe identifie les catégories de sous-traitants engagés par Secutec pour le traitement des données personnelles des clients dans le cadre du contrat.

Secutec utilise un modèle technologique indépendant des fournisseurs et à la pointe de la technologie, et peut faire appel à différents sous-traitants en fonction des services achetés, des modules activés, des configurations spécifiques aux clients et de l'évolution des technologies de cybersécurité au fil du temps.

2 Sous-traitants de l'infrastructure centrale

Secutec s'appuie sur des fournisseurs d'infrastructure cloud et d'hébergement pour fournir des composants de plateforme, des pipelines de journaux, du stockage et de la capacité de calcul.

Ces sous-traitants fournissent des services d'hébergement, de stockage et de disponibilité sécurisés et sont sélectionnés en fonction de leurs certifications de sécurité, de leur conformité et de leur disponibilité régionale.

Le traitement s'effectue principalement au sein de l'Espace économique européen lorsque cela est possible sur le plan opérationnel. Lorsque le traitement en dehors de l'EEE est nécessaire, des garanties appropriées sont appliquées conformément à l'accord de traitement des données et aux lois applicables en matière de protection des données.

3 Sous-traitants de la plateforme MySecutec et de l'application mobile

La plateforme SecureSIGHT et l'application mobile s'appuient sur des fournisseurs d'infrastructure, d'analyse et de services mobiles pour fournir l'authentification, les tableaux de bord, les notifications et les fonctionnalités de l'application.

Ces sous-traitants traitent uniquement les données personnelles au niveau de la plateforme, comme décrit à l'annexe A, et ne traitent pas les données de sécurité opérationnelle générées par les services, sauf accord explicite.

Les informations concernant les catégories de sous-traitants engagés sont mises à disposition conformément à l'article 7 de la DPA.

4 Sous-traitants SecureDNS

SecureDNS s'appuie sur des fournisseurs d'infrastructure, des composants de résolution DNS et des moteurs d'analyse de sécurité pour fournir des services de sécurité DNS.

Les sous-traitants traitent les métadonnées DNS et les données de télémétrie de sécurité nécessaires à la détection, au filtrage et au signalement des menaces, conformément au Contrat et aux garanties applicables.

5 Sous-traitants SecureSIGHT (modules)

Les modules SecureSIGHT peuvent s'appuyer sur des fournisseurs de technologies tiers pour fournir des fonctionnalités spécifiques, telles que des moteurs de détection, des renseignements sur les menaces, des services de corrélation ou d'enrichissement.

Ces sous-traitants traitent des métadonnées limitées liées à la sécurité conformément au Contrat.

Les sous-traitants applicables dépendent des modules activés et de la configuration du client et peuvent être mis à jour conformément à l'article 7 de l'ATP.

6 Sous-traitants spécifiques au client

Lorsque le client demande ou active des intégrations avec ses propres fournisseurs (par exemple, XDR, SIEM, Darknet intel, connecteurs AD fournis par le client) :

- ces outils tiers peuvent fonctionner en tant que sous-traitants ou contrôleurs distincts,
- Le client est tenu de s'assurer que ses accords avec ces fournisseurs autorisent Secutec à accéder aux données et à les traiter.

Secutec n'assume aucune obligation envers les fournisseurs sélectionnés par le client.

7 Changements de sous-traitants

Les sous-traitants peuvent être mis à jour conformément à l'article 7 de l'ADP.

Le client reconnaît que les technologies de cybersécurité évoluent en permanence et que Secutec peut ajouter, remplacer ou supprimer des sous-traitants afin de maintenir la qualité, la sécurité et la conformité du service.

8 Liste indicative des sous-traitants actuels

La liste suivante fournit **des exemples de sous-traitants actuellement utilisés** dans le cadre de la fourniture des services Secutec.

Cette liste est indicative et non exhaustive. Les sous-traitants peuvent évoluer au fil du temps conformément à l'article 7 du présent ATD.

Catégorie	Exemples de sous-traitants	Finalité
Infrastructure cloud	OVHcloud	Hébergement sécurisé des composants de la plateforme Secutec
Infrastructure / Hébergement d'applications	DigitalOcean	Hébergement des services de la plateforme
Fournisseurs de technologies de cybersécurité	SentinelOne	Moteur de sécurité XDR
Services d'applications mobiles	OneSignal	Services de notifications push
Surveillance des applications	Sentry	Surveillance et diagnostic des erreurs
Analyses	Google Firebase	Analyse de la plateforme et diagnostic des plantages

Annexe D – Principes de conservation

1 Principes de conservation

Les périodes de conservation définies dans la présente annexe sont indicatives et basées sur les nécessités opérationnelles, les exigences en matière de prestation de services et les pratiques du secteur en matière de services de cybersécurité.

Les périodes de conservation peuvent varier selon la catégorie de données et sont définies conformément aux politiques internes de conservation de Secutec et à la documentation contractuelle applicable.

Si nécessaire, les périodes de conservation peuvent être ajustées d'un commun accord entre les parties.

2 Objet et champ d'application

La présente annexe décrit les durées de conservation par défaut applicables aux données personnelles du client traitées par Secutec dans le cadre du contrat.

Ces durées de conservation s'appliquent sauf si une durée différente est explicitement convenue dans un Bon de commande ou un Cahier des charges, ou si une durée de conservation plus longue est requise ou autorisée par la loi applicable.

Secutec supprime ou anonymise les données personnelles du client après l'expiration des périodes de conservation applicables, conformément à l'article 12 de l'accord sur le traitement des données.

3 Principes généraux

Les données personnelles ne sont conservées que pendant la durée nécessaire à la détection, la surveillance, l'investigation, le signalement, l'auditabilité et la continuité du service.

Les durées de conservation sont déterminées en fonction des nécessités opérationnelles, des obligations légales et des pratiques reconnues dans le secteur en matière de cybersécurité et de services de sécurité gérés.

Lorsque les données personnelles ne sont plus nécessaires à ces fins, elles sont supprimées ou anonymisées de manière irréversible conformément à la présente annexe.

4 Plateforme SecureSIGHT et application mobile

Les données personnelles liées à la plateforme, y compris les données des comptes utilisateurs, les journaux d'authentification, les métadonnées d'accès, les communications d'assistance et les diagnostics d'application, sont conservées pendant la durée nécessaire pour assurer le fonctionnement, l'assistance, la sécurité et l'auditabilité de la plateforme.

Les périodes de conservation peuvent varier en fonction de la catégorie de données et sont définies conformément aux politiques de conservation internes de Secutec et à la documentation contractuelle applicable.

5 SecureDNS

SecureDNS traite les métadonnées des requêtes DNS, les événements de sécurité, les classifications des risques et les données de rapport nécessaires à la fourniture de services de sécurité DNS.

Les données DNS opérationnelles sont conservées pendant une période limitée nécessaire à l'analyse de la sécurité, à l'enquête sur les incidents et à la création de rapports.

Les données de rapport agrégées et les artefacts liés aux incidents peuvent être conservés pendant une période plus longue afin de faciliter la création de rapports sur les services, les enquêtes et les obligations envers les clients.

6 Modules SecureSIGHT

Les modules SecureSIGHT, y compris, mais sans s'y limiter, XDR, Leaked Credentials & Darknet Monitoring, Active Threat Hunting, Microsoft 365 Monitoring, Third-Party Risk Management et Attack Surface Management, traitent les métadonnées, les alertes, les conclusions et les informations contextuelles liées à la sécurité.

Ces données ne sont conservées que pendant la durée nécessaire pour soutenir la prestation de services, les enquêtes, les rapports et les obligations de conformité, conformément aux politiques de conservation internes de Secutec et à la documentation contractuelle applicable.

7 Conseil, tests d'intrusion et réponse aux incidents

Les données générées dans le cadre des services de conseil, de tests d'intrusion et de réponse aux incidents sont conservées pendant la durée nécessaire à la fourniture des services convenus, à l'appui des enquêtes, des rapports et de l'examen post-incident.

Si nécessaire, ces données peuvent être conservées pendant une période plus longue afin de respecter les obligations légales, réglementaires ou contractuelles, ou jusqu'à la clôture du dossier, plus une période raisonnable après la clôture.

8 Backups

Les copies de sauvegarde peuvent être conservées pendant une période limitée, conformément au calendrier standard de rotation des sauvegardes de Secutec.

Les sauvegardes contiennent des copies cryptées des systèmes de production et ne peuvent être modifiées ou supprimées de manière sélective.

9 Suppression après résiliation du contrat

Après la résiliation du Contrat, Secutec supprimera ou anonymisera les Données personnelles du Client dans un délai raisonnable, sauf dans les cas suivants :

- une période de conservation plus longue est requise ou autorisée par la loi applicable ;
ou
- les données persistent dans des sauvegardes cryptées jusqu'à ce qu'elles soient écrasées conformément aux calendriers de rotation des sauvegardes standard.

Les périodes de conservation peuvent être prolongées si nécessaire pour établir, exercer ou défendre des droits en justice.

Lorsque cela est techniquement et juridiquement possible, Secutec peut se conformer aux demandes raisonnables des clients visant à supprimer prématurément des ensembles de données spécifiques.