

Data Processing Agreement

Version 1.1 - August 2026

This Data Processing Agreement (“**DPA**”) is entered into between:

- 1) **The Customer**, acting as **Controller**; and
- 2) **Secutec BV**, a company incorporated under Belgian law, with registered office at Boomsesteenweg 41/11, 2630 Aartselaar, Belgium, company number 0875.719.463 (“**Secutec**”), acting as **Processor**.

Customer and Secutec are each a “**Party**” and together the “**Parties**”.

This DPA forms an integral part of the Agreement between the Parties and governs the Processing of Personal Data by Secutec on behalf of the Customer.

1 Definitions

All capitalised terms not defined herein shall have the meaning given in the Agreement.

- “**Affiliate**” means any entity controlling, controlled by or under common control with a Party.
- “**Agreement**” means the agreement between Customer and Secutec for the provision of Secutec’s products and services.
- “**Customer Personal Data**” means Personal Data Processed by Secutec as Processor on behalf of the Customer under the Agreement.
- “**Data Protection Laws**” means the GDPR and all applicable Belgian and EU legislation supplementing or implementing it.
- “**Data Subject Request**” means a request from a Data Subject to exercise rights under the GDPR.
- “**Subprocessor**” means any third party engaged by Secutec to Process Customer Personal Data.
- Terms such as “**Controller**”, “**Processor**”, “**Processing**”, “**Personal Data**”, “**Personal Data Breach**”, “**Supervisory Authority**”, etc. have the meaning given in the GDPR.

2 Scope of the DPA

This DPA applies to all Processing performed by Secutec in relation to the Services used by the Customer. The Processing activities that apply to all Customers, regardless of which Services they purchase, are described in **Annex A – SecureSIGHT Platform & Mobile App**.

In case of conflict between this DPA and any other contractual document, this DPA prevails with respect to data protection matters. This DPA governs the Processing of Customer Personal Data only. Processing of anonymized or aggregated data that no longer relates to an identifiable individual falls outside the scope of this DPA.

3 Roles of the Parties

The Customer acts as Data Controller and determines the purposes and means of the Processing of Customer Personal Data under the Agreement.

Secutec acts as Data Processor and processes Customer Personal Data solely on documented instructions from the Customer, unless required to do otherwise by applicable law.

Where Secutec processes aggregated and/or anonymized data that cannot reasonably be re-identified, taking into account available means, cost, time and technology, Secutec acts as an independent Data Controller for purposes such as threat intelligence, statistical analysis, service optimization, security research, and platform analytics.

Such Processing is governed by Secutec's own privacy notice and does not involve Customer Personal Data within the meaning of this DPA.

4 Documented Instructions

Secutec shall Process Customer Personal Data strictly in accordance with the Customer's documented instructions, unless required otherwise by EU or Member State law. If Secutec considers that an instruction violates Data Protection Laws, Secutec shall notify Customer and may suspend the relevant Processing.

Secutec shall not be obliged to assess whether the Customer's use of the Services complies with Data Protection Laws.

5 Confidentiality

Secutec shall ensure that all persons authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations, whether contractual or statutory.

6 Security Measures

Secutec shall implement and maintain the technical and organizational security measures described in **Annex B – Technical and Organizational Security Measures**, which apply to all Processing under this DPA.

Customer acknowledges that these measures provide a level of security appropriate to the risk, taking into account the state of the art, costs of implementation and nature of Processing (Art. 32 GDPR).

7 Subprocessing

7.1 General Authorisation

The Customer grants Secutec a general authorisation to engage Subprocessors for the Processing of Customer Personal Data in connection with the Services.

Annex C - Subprocessors describes, at a categorical level, the types of Subprocessors that may be engaged by Secutec, without listing individual vendors, reflecting the vendor-agnostic and evolving nature of cybersecurity technologies. For transparency purposes, Secutec maintains an indicative Subprocessor List describing examples of subprocessors currently used in the delivery of its services.

This list is provided for informational purposes only and does not form part of this Data Processing Agreement. The Subprocessor List may be updated from time to time to reflect technological evolution, infrastructure changes or service improvements.

Subprocessors are engaged and governed in accordance with the principles set out in this Article 7 and Annex C (Subprocessors).

Secutec may appoint, replace, or remove Subprocessors as required to deliver the Services, maintain security, ensure service continuity, or comply with applicable legal or regulatory requirements.

7.2 Notification & Objection

Secutec shall make information available to the Customer regarding changes to the categories of Subprocessors engaged for the Processing of Customer Personal Data.

The Customer may object to such changes on reasonable and documented grounds relating to data protection, taking into account the nature of the Services and the role of Subprocessors within Secutec's security operations.

Where an objection is raised, the Parties shall discuss the matter in good faith. If no reasonable alternative can be agreed, the Customer may terminate only the affected portion of the Services, without any right to damages, indemnities, or penalties related to such termination.

Changes required for security, incident response, service continuity, or compliance reasons may be implemented immediately. In such cases, Secutec shall inform the Customer without undue delay.

7.3 Subprocessor Obligations and Liability

Secutec shall ensure that any Subprocessor engaged is subject to data protection obligations that are no less protective than those set out in this DPA, including appropriate technical and organisational security measures.

Secutec remains fully liable for the performance of its Subprocessors in accordance with this DPA, to the same extent as if the Processing were carried out directly by Secutec.

Secutec remains fully liable for the actions and omissions of its Subprocessors to the same extent as if performing the Processing itself.

8 International Data Transfers

Personal Data relating to EU-originated traffic is primarily processed within the European Union.

Where Processing outside the European Economic Area is required for the provision of the Services, such transfers shall be carried out in accordance with applicable Data Protection Laws and subject to appropriate safeguards, including Standard Contractual Clauses or other valid transfer mechanisms.

9 Assistance to Customer

Secutec shall assist Customer, insofar as reasonably possible, with:

- responding to Data Subject Requests; Secutec shall not respond directly to any Data Subject Request, unless expressly instructed by Customer to do so.
- complying with Articles 32 to 36 GDPR (security, breach notification, DPIA, prior consultation).

Secutec may charge reasonable costs where assistance exceeds normal service levels, provided that Secutec informs Customer in advance of such costs.

Such assistance does not include performance of legal assessments, fulfilment of Customer's own statutory obligations, or implementation of organizational measures within the Customer's environment.

10 Audit Rights

Customer may conduct audits to verify Secutec's compliance with this DPA, subject to:

- 60 days' prior written notice;
- a maximum of one audit per 12 months;

- audits conducted during normal business hours;
- no access to Secutec's internal financial information, data of other customers, internal audit reports or trade secrets;

As an alternative, Secutec may satisfy audit obligations by providing recent ISO 27001 certificates or external ISO 27001 audit summaries.

Customer shall ensure that any audit does not unreasonably disrupt Secutec's business operations and does not involve auditors who are direct competitors of Secutec

11 Personal Data Breach Notification

Secutec shall notify Customer without undue delay upon becoming aware of a Personal Data Breach affecting Customer Personal Data.

Notification shall include the nature of the Breach, the categories of data affected, the likely consequences, and measures taken or proposed to address the Breach.

Customer remains responsible for any notifications to Supervisory Authorities and Data Subjects, unless otherwise agreed. The Customer shall notify Secutec without undue delay after becoming aware of any security incident that:

- affects Personal Data for which Secutec acts as Processor; or
- affects any confidential information, credentials, access tokens, evidence files, reports, or other data provided by Secutec to the Customer.

Such notification shall include, to the extent known, a description of the nature of the incident and its potential impact on Secutec's data or systems.

Nothing in this clause requires the Customer to notify Secutec of Personal Data Breaches for which the Customer is Controller unless Secutec's data or systems are affected.

12 Return and Deletion of Personal Data

Upon termination of the Agreement, Customer Personal Data shall be retained only for as long as necessary in accordance with the retention principles and applicable retention periods defined in Annex D – Retention Principles, unless a longer retention period is required by applicable law or agreed in writing.

Upon expiry of the applicable retention periods, Secutec shall delete or anonymize Customer Personal Data within a reasonable timeframe, except for encrypted backups which are overwritten in accordance with Secutec's standard backup rotation schedule.

Customer may request return of Personal Data before deletion.

13 Liability

The liability provisions of the Agreement apply equally to this DPA.

Nothing in this DPA restricts the rights of Data Subjects under Article 82 GDPR.

14 Governing Law and Jurisdiction

This DPA is governed by Belgian law.

Disputes shall be submitted to the exclusive jurisdiction of the courts of Antwerp.

15 Hierarchy

In case of inconsistency:

1. This DPA prevails over the Agreement;
2. Annexes prevail over this DPA to the extent they describe service-specific Processing.

In all other respects, the provisions of this DPA prevail over any conflicting terms in an Annex.

For the avoidance of doubt, Annexes describing Processing activities, Subprocessors, or retention principles shall be interpreted in accordance with and subject to the governing provisions of this DPA.

This DPA shall remain in force for as long as Secutec Processes Customer Personal Data under the Agreement.

16 Structure of Annexes

The following annexes form an integral and inseparable part of this Data Processing Agreement:

Annex A – SecureSIGHT Platform & Mobile App

Describes the Processing activities inherent to the SecureSIGHT platform and mobile application, which apply to all Customers regardless of which Services they purchase.

Annex B – Technical and Organizational Security Measures (TOMs)

Sets out Secutec's ISO27001-aligned security controls applicable to all Processing under this DPA.

Annex C – Subprocessors

Describes, at a categorical level, the types of Subprocessors that may be engaged by Secutec in the provision of the Services, in accordance with the general authorization model set out in Article 7

Annex D – Retention Principles

Describes default retention periods for the Processing of Customer Personal Data across all Services.

Annex A – SecureSIGHT Platform & Mobile App

This Annex describes the Processing of Personal Data carried out through the SecureSIGHT web platform and the MySecutec Mobile App (together, “**the Platform**”). The Platform provides authentication, user management, dashboards, alerts and access to Secutec’s Services.

This Annex applies to all Customers, regardless of which Services they purchase, as all Customers use the Platform for access and account management.

Terms not defined here have the meaning given in the DPA.

1 Scope of the processing

The Platform serves as the unified access layer for all Secutec modules.

The Platform processes user-related, authentication, technical and access data, while the underlying modules process operational cybersecurity data.

The Platform does not make independent decisions about the operational security data; they only display it.

Secutec processes only the minimum amount of Personal Data and technical data required to provide access to and functionality of the Platform, including authentication data, access logs, and operational metadata, strictly limited to service delivery, support, security, and auditability purposes.

2 Roles of the Parties

2.1 Processor role

Secutec acts as Processor for Personal Data required to provide Customers with access to, and functionality of, the Platform, including:

- User accounts
- Authentication and access control
- Logging and session metadata
- Dashboard access
- Support chat

2.2 Controller role

For analytics, crash diagnostics and performance monitoring within the Platform, Secutec acts as an independent Controller.

This Processing is carried out for the purpose of:

- improving stability and performance
- troubleshooting errors or crashes
- ensuring quality of service

This Controller Processing does not involve Customer operational data.

For this Processing, Secutec's own privacy notice applies.

3 Categories of Personal Data

The Platform processes the following categories of Personal Data:

3.1 User Account Data

- Full name
- Email address
- Organisation / tenant
- User roles and permissions
- Linked modules and service configuration

3.2 Authentication & Security Data

- Email + hashed password
- MFA/OTP verification data
- Authentication timestamps
- Session identifiers
- Login attempt logs
- IP address at login

3.3 Technical & Device Data

- Device type, OS version, device model
- App version
- Browser or app metadata
- Performance metrics
- Crash diagnostics metadata
- No geolocation is collected.

3.4 Push Notification Data

The Platform may send push notifications. For this, notification tokens are processed.

3.5 Usage Data

- Screen views
- Navigation events
- Feature usage
- Session duration

3.6 Support & Communication Data

- in-App chat messages
- timestamps and sender identifiers

3.7 Purposes of the Processing

Personal Data is processed through the Platform for the following purposes:

1. User authentication and secure access
2. Role-based access control
3. Display of service dashboards and operational insights
4. Providing support and communication
5. Maintaining security, logging and auditability
6. Monitoring performance and detecting errors (Controller role)

No Personal Data is used for marketing or unrelated profiling.

4 Subprocessors

Processing activities under this Annex may involve the use of Subprocessors, as described at a categorical level in Annex C (Subprocessors).

Annex C identifies the types and categories of Subprocessors that may be engaged by Secutec in the context of the Services, without listing individual vendors.

Subprocessors may be engaged, replaced, or updated in accordance with Article 7 of the DPA, taking into account the vendor-agnostic and evolving nature of cybersecurity technologies.

5 Retention Periods

All retention periods applicable to Personal Data processed under this Annex are governed exclusively by Annex D (Retention Principles).

This Annex describes the categories of Personal Data processed through the Platform but does not define or modify retention periods.

Annex D constitutes the single source of truth for retention periods applicable to Platform-related Personal Data.

6 Security Measures

All Processing under this Annex is protected by the technical and organizational measures described in **Annex B (Security Measures)**.

These include:

- MFA
- Encryption in transit & at rest
- Secure hosting & tenant isolation
- Logging and anomaly detection
- RBAC
- Vulnerability management

7 Customer Responsibilities

Customer shall:

- ensure that its authorized users maintain secure credentials
- manage access rights and roles

- ensure lawful monitoring of employees' accounts associated with the Platform
- avoid storing unnecessary or excessive personal data in support channels
- ensure secure use of devices that access the Platform

8 Additional Notes

- The Platform is strictly B2B and not intended for consumer use.
- The App is a supplementary interface; it does not replace the full SecureSIGHT web platform.
- Impersonation features are restricted to authorized partners.

Annex B – Technical and Organizational Security Measures

Secutec implements the following technical and organizational measures (“**TOMs**”) to ensure level of security appropriate to the risk associated with the Processing of Customer Personal Data, in accordance with Article 32 GDPR.

These measures apply to all services, unless additional service measures are added in additional annexes.

1 Information Security Management System (ISMS)

1.1 ISO 27001 Framework

Secutec maintains a formal Information Security Management System (ISMS) aligned with the ISO/IEC 27001 standard.

The ISMS governs Secutec’s approach to confidentiality, integrity and availability of information assets.

1.2 Documented Policies

The ISMS is supported by a comprehensive set of documented policies, including (non-exhaustively):

- Information Security Policy
- Access Control Policy
- Network Security Policy
- Operations Security Policy
- Cryptography & Key Management Policy
- Human Resources Security Policy
- Asset Management Policy
- Business Continuity & Disaster Recovery Policy
- Physical Security Policy
- Supplier & Third-Party Management Policy
- Secure Development & Change Management Policy
- Incident Management Policy
- Compliance Policy
- ISMS Governance & Risk Assessment Policy

These internal policies are not part of the Agreement and may be updated from time to time as part of continuous improvement under ISO 27001.

1.3 Evidence of Compliance

Upon Customer request, Secutec may provide evidence of ISMS implementation such as:

- ISO/IEC 27001 certificates and scope statements,
- summary audit reports,
- compliance attestations.

Internal policy documents and sensitive operational details are not shared in full for security reasons.

2 Access Control Measures

2.1 Principle of Least Privilege

Access to Customer Personal Data is granted strictly on a need-to-know basis.

2.2 Authentication & Authorisation

Multi-factor authentication is required for administrative access.

Unique user identities are enforced.

Access rights are reviewed periodically.

2.3 Immediate Revocation

Access is revoked promptly upon role change or termination of employment.

3 Physical and Environmental Security

Customer Personal Data is primarily hosted in secure, professionally managed EEA-based datacenters of certified cloud providers.

Where processing outside the EEA is required, appropriate safeguards are applied in accordance with the DPA and applicable data protection laws.

Datacenters provide physical access control, environmental protection, fire detection, redundancy and 24/7 monitoring.

4 Encryption & Data Protection

Encryption in transit: All communication channels used to transfer Customer Personal Data are secured using TLS 1.2+ or equivalent.

Encryption at rest: Logs, DNS data and service data are encrypted at rest using industry-standard algorithms.

Cryptographic keys are managed securely.

5 Network Security

Secutec applies network segmentation, firewalls and intrusion detection/prevention systems.

DNS and service-specific traffic is monitored for anomalies and malicious activity.

Anti-DDoS protections and rate-limiting mechanisms protect service availability.

6 Operations Security

Secure coding practices and peer review are enforced for in-house developed components.

All systems undergo regular vulnerability scanning, and patches are applied according to severity.

Logging of security-relevant events is maintained centrally and monitored. Access to Customer Personal Data is logged and logs are regularly reviewed.

Backup procedures ensure data restoration capability; backups are encrypted.

7 Incident Detection & Response

Secutec maintains an Incident Response Plan aligned with ISO 27001 and NIS2 standards.

Security incidents are investigated, documented and contained promptly.

In case of a Personal Data Breach affecting Customer Personal Data, Secutec will notify the Customer without undue delay as required under Article 11 of the DPA.

8 Business Continuity & Disaster Recovery

Services are deployed primarily across redundant cloud infrastructure within the EEA.

Disaster recovery procedures are tested periodically.

Critical systems are monitored 24/7 for performance and availability.

9 Supplier & Subprocessor Management

Subprocessors are assessed for security posture before onboarding.

Only subprocessors with appropriate certifications (e.g., ISO 27001) are engaged.

Contracts with subprocessors include obligations equivalent to those imposed by the DPA.

10 Data Minimisation & Retention

Secutec shall process only the minimum amount of Personal Data and technical data required to deliver the Services in accordance with this Agreement.

Such data may include Customer-supplied data, operational security data, authentication and access data, alert metadata, and publicly available information, strictly limited to what is necessary for service delivery, investigation, reporting, and security operations.

Retention of such data is governed exclusively by Annex D (Retention Principles).

11 Testing & Continuous Improvement

Security testing is performed periodically.

Findings are tracked and remediated according to risk.

The TOMs are reviewed at least annually and updated as needed.

Annex C – Subprocessors

1 Scope

This Annex identifies the categories of Subprocessors engaged by Secutec for the Processing of Customer Personal Data under the Agreement.

Secutec operates a vendor-agnostic, best-of-breed technology model and may engage different Subprocessors depending on the Services purchased, modules activated, customer-specific configurations, and the evolution of cybersecurity technologies over time.

2 Core Infrastructure Subprocessors

Secutec relies on cloud infrastructure and hosting providers to deliver platform components, log pipelines, storage, and compute capacity.

Such Subprocessors provide secure hosting, storage, and availability services and are selected based on security certifications, compliance posture, and regional availability.

Processing primarily takes place within the European Economic Area where operationally feasible. Where processing outside the EEA is required, appropriate safeguards are applied in accordance with the DPA and applicable data protection laws.

3 MySecutec Platform & Mobile App Subprocessors

The SecureSIGHT platform and mobile application rely on infrastructure, analytics, and mobile service providers to deliver authentication, dashboards, notifications, and application functionality.

These Subprocessors process platform-level Personal Data only, as described in Annex A, and do not process operational security data generated by the Services unless explicitly agreed.

Information regarding the categories of Subprocessors engaged is made available in accordance with Article 7 of the DPA.

4 SecureDNS Subprocessors

SecureDNS relies on infrastructure providers, DNS resolver components, and security analytics engines to deliver DNS security services.

Subprocessors process DNS metadata and security telemetry required for threat detection, filtering, and reporting, in accordance with the Agreement and applicable safeguards.

5 SecureSIGHT Subprocessors (Modules)

SecureSIGHT modules may rely on third-party technology providers to deliver specific functionalities, such as detection engines, threat intelligence, correlation, or enrichment services.

Such Subprocessors process limited security-related metadata in accordance with the Agreement.

The applicable Subprocessors depend on the modules activated and the customer configuration and may be updated in accordance with Article 7 of the DPA.

6 Customer-Specific Subprocessors

Where the Customer requests or activates integrations with its own vendors (e.g., customer-provided XDR, SIEM, Darknet intel, AD connectors):

- such third-party tools may operate as Subprocessors or separate Controllers,
- the Customer is responsible for ensuring that its agreements with such vendors permit Secutec's access and Processing.

Secutec does not assume obligations toward Customer-selected vendors.

7 Subprocessor Changes

Subprocessors may be updated in accordance with Article 7 of the DPA.

The Customer acknowledges that cybersecurity technology stacks evolve continuously and that Secutec may add, replace, or remove Subprocessors to maintain service quality, security, and compliance.

8 Illustrative List of Current Subprocessors

The following list provides **examples of subprocessors currently used** in the provision of Secutec services.

This list is indicative and non-exhaustive. Subprocessors may evolve over time in accordance with Article 7 of this DPA.

Category	Example Subprocessors	Purpose
Cloud Infrastructure	OVHcloud	Secure hosting of Secutec platform components
Infrastructure / Application Hosting	DigitalOcean	Hosting of platform services
Cybersecurity Technology Providers	SentinelOne	XDR security engine
Mobile Application Services	OneSignal	Push notification services
Application Monitoring	Sentry	Error monitoring and diagnostics
Analytics	Google Firebase	Platform analytics and crash diagnostics

Annex D – Retention Principles

1 Retention Principles

Retention periods defined in this Annex are indicative and based on operational necessity, service delivery requirements, and industry practices for cybersecurity services.

Retention periods may vary by data category and are defined in accordance with Secutec's internal retention policies and applicable contractual documentation.

Where required, retention periods may be adjusted by mutual agreement between the Parties.

2 Purpose and Scope

This Annex describes the default retention periods applicable to Customer Personal Data Processed by Secutec under the Agreement.

These retention periods apply unless a different period is explicitly agreed in an Order Form or Statement of Work, or a longer retention period is required or permitted by applicable law.

Secutec deletes or anonymises Customer Personal Data after expiry of the applicable retention periods in accordance with Article 12 of the DPA.

3 General Principles

Personal Data is retained only for as long as necessary to support detection, monitoring, investigation, reporting, auditability, and service continuity.

Retention periods are determined based on operational necessity, legal obligations, and recognized industry practices for cybersecurity and managed security services.

Where Personal Data is no longer required for these purposes, it is deleted or irreversibly anonymized in accordance with this Annex.

4 SecureSIGHT Platform & Mobile App

Platform-related Personal Data, including user account data, authentication logs, access metadata, support communications, and application diagnostics, is retained for the duration necessary to provide platform functionality, support, security, and auditability.

Retention periods may vary depending on the data category and are defined in accordance with Secutec's internal retention policies and applicable contractual documentation.

5 SecureDNS

SecureDNS processes DNS query metadata, security events, risk classifications, and reporting data required to deliver DNS security services.

Operational DNS data is retained for a limited period necessary for security analysis, incident investigation, and reporting.

Aggregated reporting data and incident-related artefacts may be retained for a longer period to support service reporting, investigation, and customer obligations.

6 SecureSIGHT Modules

SecureSIGHT modules, including but not limited to XDR, Leaked Credentials & Darknet Monitoring, Active Threat Hunting, Microsoft 365 Monitoring, Third-Party Risk Management, and Attack Surface Management, process security-related metadata, alerts, findings, and contextual information.

Such data is retained only for as long as necessary to support service delivery, investigation, reporting, and compliance obligations, in accordance with Secutec's internal retention policies and applicable contractual documentation.

7 Consultancy, Pentesting & Incident Response

Data generated in the context of consultancy, penetration testing, and incident response services is retained for the duration necessary to deliver the agreed services, support investigation, reporting, and post-incident review.

Where required, such data may be retained for a longer period to support legal, regulatory, or contractual obligations, or until case closure plus a reasonable post-closure period.

8 Backups

Backup copies may persist for a limited period in accordance with Secutec's standard backup rotation schedule.

Backups contain encrypted copies of production systems and cannot be selectively altered or purged.

9 Deletion After Contract Termination

Following termination of the Agreement, Secutec shall delete or anonymize Customer Personal Data within a reasonable timeframe, except where:

- a longer retention period is required or permitted by applicable law; or
- data persists in encrypted backups until overwritten in accordance with standard backup rotation schedules.

Retention periods may be extended where necessary to establish, exercise, or defend legal claims.

Where technically and legally feasible, Secutec may comply with reasonable customer requests for early deletion of specific data sets.