SERVICE-related description

SOC as a Service

Version 1.4 (23.09.2025)

1. Designation and object of SERVICE

1.1 Object of Service:

The SERVICE relates to services in the area of „SOC as a Service “.

1.2 Purpose, Scope and Type of the Service:

The parties agree on the type and scope as well as the exclusive purposes of the commissioned data processing of the data by the contractor as follows:

The contractor performs data processing as part of the technical and administrative services for the provision and operation of a Security Operation Center (SOC). The SOC is the central organizational unit for detecting and responding to security incidents in the connected sources. To optimize and automate security processes, the contractor uses a SOAR (Security Orchestration, Automation, and Response) tool that enables efficient coordination between the various security systems, performs automated responses to incidents, and supports the documentation of actions. The connected sources include, but are not limited to, a SIEM (including UEBA), an EDR/XDR (including Anti-Virus), an NGFW or an IDS/IPS. The sources connected to the SOC depend on the client's request.

To enrich and contextualize security-relevant events, the contractor also uses threat intelligence platforms. These enable the correlation and analysis of threat information from the various sources, thus supporting decision-making in the SOC and the prioritization of measures.The contractor also performs data processing on behalf of the client according to the service description for the following purposes:

- Security Monitoring (Level 1 & 2)
- Alerting and Event Management
- Threat Hunting
- Security Incident Response Support
- Source Monitoring

1.3 Type of Data:

Commissioned Data Processing relates to the following types of data:

The types of data processed in the context of service provision cannot be precisely defined in advance. The types of data depend on the sources connected to the SOC, the client's requests, and the personal data provided by the client in each individual case.

As part of the provision of services, the following categories of data are processed in any case - but not exhaustively:

- Master and contact data (e.g. name, email address)
- Login data (e.g. user name, password)
- IT usage data (e.g. log data, IP address, user ID, device ID)
- Login and logout data (successful or failed login)
- Change of permissions (audit logs) and access to tools
- Log data on access to files and resources at client, VDI and server level (e.g. information on deviations/blocks/failed access, time of access)
- Connection data (e.g. proxy logs, VPN logs, firewall logs)

Special categories of data[1]:

☐ The Commissioned Data Processing does not concern any special categories of data within the meaning of Art. 9 GDPR.

☒ The Commissioned Data Processing concerns the following special categories of data within the meaning of Art. 9 GDPR:

It cannot be ruled out in advance that special categories of personal data may be processed by the contractor in the context of an incident response, if special categories of personal data are located on the isolated host/client.

1.4 Categories of data subjects concerned by the commissioned data processing

The data concerns the data of the following categories of data subjects:

The categories of data subjects depend on the client's sources connected to the SOC. For example, it is possible, that personal data of the client’s employees or customers may be processed.

[1] Special categories of personal data include: Data revealing the ethnic origin, political opinions, religious or philosophical beliefs or trade union membership as well as genetic data, biometric data, health data and data relating to sex life or sexual orientation.

2. Designation of subcontractors

☐ No subcontractors are used as part of the Commissioned Data Processing.

☒ In accordance with section 8 of the FRAMEWORK AGREEMENT on the Commissioned Data Processing, the subcontractors listed below are used as part of the Commissioned Data Processing.

The following subcontractors process the data on behalf of the contractor for partial SERVICES of the Commissioned Data Processing:

Designation of subcontractor	Address Subcontractor	Description of the Commissioned Data Processing
Cyfidelity Security Services GmbH	Bechterdisser Straße. 10 33719 Bielefeld	▪ Security services for detecting, analysing and defending against IT security threats – for example in the area of digital forensics and incident response
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay Dublin 2 Ireland	▪ Provision and operation of Google SOAR and other SecOps services on Google Cloud Platform ▪ Manufacturer Support and Troubleshooting
NoVirusThanks Company Srl	VIA CANNAVA 86 43043 Borgo Val Di Taro Perugia Italien	▪ Provision and operation of the threat intelligence platform APIVoid
OEDIV Romania SRL	UNITED BUSINESS CENTER 0 TIMIȘOARA S.R.L. Timișoara, 2 Piața Consiliul Europei square, Iulius Town, Timiș County Building 03, 3rd floor Postal Code: 300627	▪ Business support activities

3. List of permitted Commissioned Data Processing activities in third countries

☐ No data processing takes place within the scope of the Commissioned Data Processing in third countries.

☒ In accordance with Section 2 of the FRAMEWORK AGREEMENT, the Client consents to the Contractor and/or subcontractors in the third countries specified below to carry out parts of the Commissioned Data Processing:

Designation of subcontractor	Description of the Commissioned Data Processing provided in third countries	Third country designation
Google Cloud EMEA Limited	▪ Provision and operation of Google SOAR and other SecOps services on Google Cloud Platform ▪ Manufacturer Support and Troubleshooting	▪ **Provision and operation of Google SOAR and other SecOps services on Google Cloud Platform** The Data Center Location EU was chosen for the provision and operation of the Google SOAR and other SecOps services on the Google Cloud Platform. As part of the operation of these services, data may be transferred to third countries due to the use of additional subcontractors. The current list of Google Cloud Platform subcontractors can be viewed at Google Cloud Platform Subprocessors | Google Cloud. The list of subcontractors used specifically for the SecOps services can be viewed at SecOps Services Subprocessors | Google Cloud. ▪ **Manufacturer Support and Troubleshooting** Manufacturer support and troubleshooting of Google Cloud Platform can be provided by Google's subcontractors in various third countries, depending on the type and scope of the support services as well as the respective support times. As part of these support services, Google's subcontractors do not have direct access to stored customer data. Further information on the subcontractors used can also be

		found under the following link: Google Cloud Platform Subprocessors | Google Cloud Data transfers to third countries are carried out in compliance with the applicable data protection regulations and are secured by suitable guarantees in accordance with Art. 44 ff. GDPR. Comprehensive information on data protection in the Google Cloud can be found at Datenschutz-Center | Google Cloud The scope of the Google Compliance Programs for the SecOps Services can be viewed at SecOps Services in Scope by Compliance Program | Google Cloud
NoVirusThanks Company Srl	▪ Provision and operation of the threat intelligence platform APIVoid	As part of the provision and operation of the threat intelligence platform APIVoid, personal data is transferred to the USA. The data transfer takes place within the framework of the applicable data protection regulations, in particular taking into account suitable safeguards in accordance with Art. 44 ff. GDPR.

4. Additional arrangements on SERVICE-related technical and organisational measures

☒ As part of the provision of the services, the Contractor shall take the technical and organisational measures defined in ANNEX 2 of the FRAMEWORK AGREEMENT to ensure the security of the Commissioned Data Processing in accordance with Art. 32 GDPR.

☐ In addition to the technical and organisational measures defined in ANNEX 2 of the FRAMEWORK AGREEMENT, the contractor shall take the technical and organisational measures described below as part of the provision of the SERVICES to ensure the security of the Commissioned Data Processing in accordance with Art. 32 GDPR.

Description of SERVICE-related technical and organizational measures:

☐ Instead of the technical and organisational measures defined in ANNEX 2 of the FRAMEWORK AGREEMENT, the contractor shall take the technical and organisational measures described below as part of the provision of the SERVICES to ensure the security of the Commissioned Data Processing in accordance with Art. 32 GDPR.

Description of SERVICE-related technical and organizational measures: