Full Coverage - Subscription and Support Terms

Last Modified: 2021-Sept-20

In addition to the software licence, which runs from activation until the purchased duration, Swarm Analytics offers support plans designed to meet maintenance needs and enhance the quality and stability of operating the products. The package is called Full Coverage and consists of three components

1. Software Subscription
2. Support
3. Advanced Replacement (for hardware or hardware bundle products)

Definitions

Software Subscription	During active Full Coverage period the customer is entitled to receive all software bugfixes, updates and upgrades, which is released by Swarm Analytics for the respective product
Support	During active Full Coverage period the customer is entitled to contact Swarm Analytics Support according to the guidelines set forth
Advanced Replacement	During active Full Coverage period the customer is entitled to get hardware replacement, if it is broken.
General request	= The customer has general questions about the products or services of Swarm Analytics.
Moderate incident	= The system is still working, but the full functionality of the system is degregated
Critical incident	= The application cannot be used due to a malfunction of the hard or software delivered and maintained by Swarm Analytics
Communication channel	= Email, Phone
Support Times	Austrian business days - 5 days a week 8 hours (09:00-17:00 MEZ)
Response Time	= Period - ***within the support times*** - between receipt of the customer inquiry via a communication channel and the first feedback by a support employee of the Swarm Analytics
Start with problem solving within specified period	= Period - ***within the support times*** - between receipt of the customer request via a communication channel and the time at which a support employee of Swarm Analytics begins to solve the problem.

Standard support

To ensure high performance of your solution, Swarm Analytics offers a Standard Support plan that meet the needs of many enterprises. Standard coverage applies to both hardware and software products, since each often must work together as a total solution.
Swarm Analytics is not liable for errors in the delivery of the customer request via the selected communication channel. The categorization of the support requests is carried out by the employees of Swarm Analytics.

Standard coverage includes

- Support via Email, Phone during support times
- Remote support
- Access to the Swarm Analytics Web Knowledge Base

Hardware Support – Advanced Replacement (for hardware or hardware bundle products)

Duration

The Advanced Replacement service begins on the date the Swarm Analytics product is activated and expires when the Swarm Subscription expires.

If you purchased your product directly from Swarm Analytics, Inc:

During your Advanced Replacement service period, if your product fails, you should contact Swarm Analytics. We will use commercially reasonable efforts to ship a replacement product within 1 business day (for EEA only). For customers outside the EEA, we will use commercially reasonable efforts to ship a replacement product via express mail within one business day after receiving the request. Upon contacting Swarm Analytics, you must return the original product to us. We will issue a Return Material Authorization Number for you to include with the return and will require a valid credit card number or purchase order. We will not charge you for the replacement product as long as you return the original product to us within 30 days after shipment of the replacement product. If we do not receive the original product within 30 days, we will charge your credit card or process the purchase order at the current list price for that product. Swarm Analytics will pay all shipping costs for the replacement product, provided you reside in the EEA. The customer is responsible for shipping costs back to Swarm Analytics of the covered unit.

If you purchased your product from a reseller:

During the Advanced Replacement Service period, if your product fails, you should contact your Reseller. Your Reseller will coordinate the shipment of a replacement product to you within 1 business day after receiving the request (for EU only). Upon contacting your Reseller to request a replacement product, you must return the original product. Your Reseller will coordinate the issuance of a Return Material Authorization Number for you to include with the return. A valid credit card number or purchase order

will be required at the time of issuing the Return Material Authorization Number. You will not be charged for the replacement product as long as you return the original product within 30 days after shipment of the replacement product. If the original product is not received within 30 days, your credit card will be charged or the purchase order will be processed at the current list price for that product. Swarm Analytics will pay all shipping costs for the replacement product, provided you reside in the EU. Alternatively, you may contact Swarm Analytics directly to coordinate the replacement and return of the original product, provided you have not already contacted your Reseller.

The Advanced Replacement Service does not cover:

- External causes such as abuse, misuse or problems with electrical power
- Servicing not authorized by Swarm Analytics
- Usage that is not in accordance with product instructions
- Failure to follow the product instructions or failure to perform preventive maintenance
- Problems caused by using accessories, parts, or components not supplied by Swarm Analytics
- Products with missing or altered serial numbers
- Products for which Swarm Analytics has not received payment
- Products that have been physically damaged

Premium Support

For customers with critical infrastructure we offer a special support package for our products with our service level agreement, providing you reliable service that helps you to control your costs.

Premium coverage includes

- Standard support coverage
- Critical incident: Start with problem solving within 6 hours during support times
- Moderate incident: Start with problem solving within 24 hours during support times
- General request: Response time within 24 hours during support times

Standard and Premium support does not include on-site support. Expenses (hotel and travel expenses, export/ import duties and hours of work 140€/h) will be charged separately.

Support Contact

Phone: +43 (0) 664 4678233 (subject to change)

Email: support@swarm-analytics.com

Office hours: 08:00-18:00 CET on Austrian business days

Data Protection and GDPR Compliance

The Customer is responsible for personal data processed by the Customer in the Swarm Analytics Applications (data controller).
Within the scope of the Support Agreement, Swarm Analytics shall carry out maintenance and/or servicing work on the Customer's IT systems, including the Swarm Analytics Applications.

In this context, it cannot be excluded that Swarm Analytics processes personal data in order to carry out or be able to carry out the maintenance and care of IT systems of the Customer.

According to Art 28 GDPR, it is therefore necessary for the customer and Swarm Analytics to conclude a data processing agreement. This data processing agreement is an annex to the Support Agreement.

Annex

Data Processing Agreement (DPA)

closed between

Swarm Analytics GmbH
Helga-Krismer-Platz 1
6020 Innsbruck
Austria

hereinafter referred to as "Data Processor"

and

Client

hereinafter referred to as "Data Controller" or "Client".

1. General

Between Data Processor and Data Controller Parties exists a contract regarding the maintenance and servicing of IT systems of Data Controller ("Supporting Agreement").

This Data Processing Agreement (DPA) is made between the parties as a supplementary regulation for compliance with the data protection regulations of Art 28 of the General Data Protection Regulation (GDPR).

The Data Processor carries out maintenance and/or servicing work on the client's IT systems on behalf of the client as Data Controller. In this context, it is not excluded that the Swarm Analytics processes personal data in order to carry out or be able to carry out the maintenance and care of IT systems.

2. Duration and termination of data processing

This Data Processing Agreement is effective from the moment of its acceptance by the Client and ends upon termination of the Supporting Agreement.

After termination of this contract, the Data Processor must return all processing results and documents containing data to the Client or destroy them.

3. Subject of the data processing

According to the Support Agreement, the Client's order to the Data Processor includes the following work and/or services:

- Support in setting up and configuring Swarm Control Center
- Support in setting up and configuring Swarm Perception Boxes
- Support in performing software updates of Swam Control Center and Perception Boxes
- The contract may also involve the processing of the following types of personal data:
- Still photos from video streams with persons and vehicles
- Video streams with persons and vehicles
- Names and emails from employees of Client
- License plate data from vehicles

4. Rights and obligations of the Data Controller

The Client has the right to issue instructions to the Data Processor at any time regarding the type, scope and procedure of the maintenance and care of IT systems. Instructions may be given in text form (e.g. e-mail). If such instructions result in additional expenses for the Data Processor, the Client shall reimburse these additional expenses appropriately.

The Client is entitled to monitor the Data Processor's compliance with the statutory provisions on data protection and/or compliance with the contractual provisions concluded between the Parties and/or

compliance with the Client's instructions at any time to the extent required. To the extent necessary to exercise these monitoring rights, the Data Processor will also provide the Client with all necessary information in this regard.

The Client is obligated to maintain confidentiality and secrecy with regard to the circumstances and data of which it becomes aware in the course of exercising the inspection rights, provided that this does not preclude the assertion of its rights under the GDPR.

The Client shall take technical measures to ensure that the Data Processor does not have access to Personal Data that is not necessary for the performance of the Support Agreement.

The Client will notify the Data Processor without delay if he discovers any errors or irregularities in connection with the maintenance and care provided by the Data Processor.

5. General obligations of the Data Processor

The Data Processor is located within the European Union (Austria) and will process personal data primarily in Austria.

When performing support services by remote access, the Data Processor will process personal data in the system of the Data Controller (Customer). In these cases, the Customer must ensure that this system is established in compliance with the GDPR.

If data processing outside the European Union is necessary (e.g. by involving sub-processors outside the EU), the Processor will ensure that the appropriate level of data protection as defined by the GDPR is safeguarded by providing suitable guarantees as defined by Art 45 or Art 46 (2) of the GDPR.

The Data Processor is obliged to design his operating procedures in such a way that the data that he processes in connection with the maintenance / service work on the order are protected from unauthorized access by third parties.

The Data Processor will also comply with his obligations under Article 30 (2) GDPR to maintain a record of all categories of processing activities carried out on behalf of a Data Controller (Client).

The Data Processor will inform the Client immediately if an instruction given by the Client violates legal regulations in its opinion. The Data Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or changed by the Client.

The Data Processor is obliged to notify the Client without delay of any infringement of data protection regulations or of the contractual agreements made and/or of the Client's instructions given which has occurred in the course of the processing of data by him or by other persons involved in the processing.

The Data Processor is informed that the Client may be subject to a notification obligation pursuant to Articles 33 and 34 GDPR in the event of a data protection breach, which provides for notification to the supervisory authority within 72 hours of becoming aware of the breach. The Data Processor will support the Client in the implementation of the notification obligations. The Data Processor will also inform the Client in particular and without delay of any unauthorised access to personal data processed on behalf of the Client.

The Data Processor is obliged to maintain confidentiality when processing data for the Client. The Processor shall also oblige its employees to maintain confidentiality about the personal data processed on behalf of the Client.

The Data Processor will support the Client in complying with the obligations set out in Art 33-36 GDPR, insofar as the Client is dependent on the Data Processor's support in this respect.

6. Sub-data processing

The Client consents to the use of further Sub-Data-Processors by the Data Processor.

The Data Processor will inform the Client of any intended change regarding the engagement or change of other Sub-Data-Processors and give the Client the opportunity to object to such changes. If a Sub-Data-Processor is removed without replacement, the Client does not have to be informed of this.

The Data Processor intends to engage only those Sub-Data-Processors who, based on the technical and organizational measures taken by them and documented towards the Data Processor, are suitable and also obliged to carry out the processing of personal data in accordance with the requirements of the GDPR.

For this purpose, the Data Processor must ensure that the Client can also assert its control rights and other rights directly against the Sub-Data-Processor to the same extent and that the Sub-Data-Processor is subject, analogously, to the same data protection obligations towards the Client as the Data Processor is subject to under this Agreement.

The sub-processor must either be established within the European Union/European Economic Area or there must be sufficient guarantees that it ensures an adequate level of protection for the data processing

as defined by the GDPR (e.g. by guarantees within the meaning of Article 46(2) of the GDPR or by a decision pursuant to Article 45(3) of the GDPR, etc.). Sub-Data-Processors are not allowed to hire other Sub-Data-Processors without the consent of the Client.

The Data Processor is required to conclude agreements with the Sub-Data-Processors within the meaning of Article 28 (4) GDPR.

7. Protection of data subjects' rights

The client is solely responsible for safeguarding the rights of the data subjects. The Data Processor will support the Client with suitable technical and organizational measures in complying with the Client's obligation to respond to requests from data subjects pursuant to Art 12-23 GDPR, insofar as the Client is dependent on the Data Processor 's support in this respect.

8. Technical and organisational measures for data security

The Data Processor undertakes towards the Client to comply with the technical and organizational measures required pursuant to Art 32 GDPR.

In the event that the Data Processor also carries out the maintenance and servicing of IT systems for the Client outside the Client's business premises (e.g. in the case of remote maintenance), the Data Processor must comply with the technical and organizational measures for the protection of personal data specified in the ANNEX to this Agreement.

9. Final provisions

This contract is subject to Austrian law.

Should individual parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

A. Terms of the Data Processor's use of sub-processors and list of approved sub-processors

A.a Terms of the Data Processor's use of sub-processors, if applicable

The Data Processor has the Data Controller's general consent for the engagement of sub-processors. The Data Processor shall, however, inform the Data Controller of any planned changes with regard to additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes. Such notification shall be submitted to the Data Controller a minimum of 3 months prior to the engagement of sub-processors or amendments coming into force. If the Data Controller should object to the changes, the Data Controller shall notify the Data Processor of this within 30 days of receipt of the notification. The Data Controller shall only object if the Data Controller has reasonable and specific grounds for such refusal.

A.b Approved sub-processors

The Data Controller shall on commencement of this Data Processing Agreement approve the engagement of the following sub-processors:

Name	VAT ID (or similar)	Address
Microsoft Österreich GmbH	ATU 15162507	A-1120 Wien Am Euro Platz 3
Microsoft Ireland Operations Limited	IE 825 39822	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18

The Data Controller shall on the commencement of this Data Processing Agreement specifically approve the use of the above sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written consent – to engage a sub-processor for 'different' processing than the one that has been agreed or have another sub-processor perform the described processing.

B. Instruction pertaining to the use of personal data

B.a Security of data processing systems

The level of security shall reflect:
That the processing may involve a large volume of personal data which are subject to Article 4 of the General Data Protection Regulation on 'personal data' which is why a 'high' level of security should be established.

The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Data Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller (on the basis of the risk assessment that the Data Controller has performed):

- In order to gain access to any service which has access to stored data, a user account within the Active Directory of the Data Processor is needed. All services are using the authentication standard provided by Microsoft Active Directory service for access.
- In order to secure the data transmission from the data controller to the data processor, Swarm is using a self hosted SFTP share, which will be created for the sole purpose of transmitting data between the parties.
- In order to secure the data while stored at the data processors premise, the data is secured through a general firewall concept, which whitelists only trusted sources and is maintained by the data processor. Also, the storage service used is authentication based and controlled by the central Active Directory of the data processor. All data is stored within Microsoft Azure based services unless stated otherwise.
- In order to have access to the stored data in remote working scenarios (e.g. home office, travel, etc.), it is needed to have an active VPN connection to the Swarm Analytics Firewall – located within the HQ. Access to any storage service is limited by an IP whitelist, which only allows access from within the internal network or the routed VPN network segment. Direct access from other public IPs other than the static HQ IP, is not possible.

B.b Processing location

Processing of the personal data under this Data Processing Agreement cannot be performed at other locations than the following without the Data Controller's prior written consent:

All processing is done within servers hosted in the EU (Location is chosen through Azure) and preference data center (if available) is Frankfurt (otherwise another data center location within the EU).

B.c Duration of storage

Personal data are stored with the Data Processor until the Data Controller requests that the data are erased or returned.