DATA PROCESSING AGREEMENT

Enterprise

This Data Processing Agreement ("**DPA**") is incorporated into and made a part of the Main Agreement (as defined below) and reflects the parties' consent with regard to the Processing of Personal Data. If the provisions of this DPA and the Main Agreement conflict, then the provisions of this DPA shall control. This DPA consists of the main body of the DPA and its exhibits.

This DPA will not become valid and legally binding if Subscriber is not a party to the Main Agreement. The parties agree that this DPA supersedes any prior data processing agreements (including any prior Data Processing Agreements).

If Subscriber has subscribed indirectly via an authorized reseller or other partner of Cyren (regardless of whether Cyren provides support and maintenance directly to Subscriber), and has entered into a DPA with such reseller or partner with respect to the Services, this DPA is not applicable to you.

Introduction/Preamble

Cyren offers to Subscriber products and services as further defined in the Main Agreement (collectively, the "**Services**") that improve the security of Subscriber's electronic communication systems. The Services are designed to detect, prevent, and manage, or assist in the detection, prevention, and managing of security threats, mass emailing and fraud attempts by exploiting within or against systems, networks, devices, files, and other data. For this purpose, Cyren scans/ reviews the electronic communication of Subscriber and hereby enables Subscriber to detect attacks on its networks by malicious software and/or fraudulent communication or dangerous e-mails (viruses, malware) or mass mailings (SPAM).

In the framework of the Processing of Personal Data by Cyren in accordance with the terms of this DPA, Subscriber's Personal Data will be subject to the following basic processing activities:

1. Providing the Services purchased by the Subscriber under and pursuant to the Main Agreement and utilizing such Service's capabilities.

2. Providing account management and customer technical Support Services

1. DEFINITIONS

a. "**Affiliate**" has the same meaning ascribed to it in the Main Agreement.

b. "**Binding Corporate Rules**" shall meaning binding corporate rules in accordance with Article 47 of the Regulation (EU) 2016/679 ("**GDPR**") which have been approved by the competent supervisory authority.

c. "**Cyren**" means the Cyren entity with whom the Main Agreement has been signed.

d. "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data Breach**", **"Process" and "Processing"** shall each have the definitions and meanings ascribed to them by the applicable Data Protection Laws, and shall include any equivalent or corresponding terms applied by such applicable Data Protection Laws (e.g., “Business” instead of “Data Controller” and “Service Provider” instead of “Data Processor” under the California Consumer Privacy Act).

e. **“DPA”** means this Data Processing Agreement.

f. “**Data Protection Laws**” means all laws and regulations applicable to the Processing of Personal Data under the Main Agreement, including such laws, by way of example and without limitation, the General Data Protection Regulation, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act.

g. “**Main Agreement**” means the Cyren End User Subscription Agreement – Europe (or other sales, license, beta, evaluation or similar agreement if applicable) including all related orders entered into between Cyren and Subscriber.

h. “**Malware**” means computer software or program code that is designed to damage or reduce the performance or security of a computer program or data.

i. “**Personal Data**” means any information relating to an identified or identifiable individual that has been provided to Cyren by Subscriber in connection with the Main Agreement.

j. “**Standard Contractual Clauses**” mean standard data protection clauses providing adequate safeguards for transfers of Personal Data to Third Countries which have been adopted by the European Commission. Once the standard data protection clauses have been amended or replaced, the amended respectively the replacing clauses will constitute the Standard Contractual Clauses.

k. “**Service(s)**” has the same meaning ascribed to it in the Main Agreement.

l. “**Spam**” means a large number of unsolicited email messages with similar content sent or received in a single operation or a series of related operations.

m. “**Sub-Processor**” means a Data Processor engaged as subcontractor by another Data Processor.

n. **“Support Service”** means technical support services in accordance with the applicable SLAs.

o. **“Subscriber**” means the party to the Main Agreement.

p. “**Third Country**” means any country, which is neither a Member State of the European Union (EU) nor a member of the European Economic Area (EEA).

q. “**Third Country Sub-Processor**” means a Sub-Processor or a sub-Sub-Processor located in a Third Country or otherwise processing Personal Data in a Third Country.

2. SCOPE

2.1 **Roles of the Parties.** The parties acknowledge and agree that with respect to the Processing of Personal Data, Subscriber is the Data Controller and Cyren is the Data Processor.

2.2 **Compliance with Data Protection Laws.** Subscriber shall comply, in all respects, with all applicable Data Protection Laws at all times during the term of this DPA, in particular with all obligations relating to the rights of Data Subjects pursuant to Art. 15-23 GDPR and all information obligations towards Data Subjects pursuant to Art. 12-14 GDPR. Subscriber's responsibilities in this respect include, but are not limited to: (i) ensuring that the instructions it provides to Cyren for the purpose of processing Personal Data comply with all applicable Data Protection Laws; (ii) ensuring that there is a lawful basis for the Processing of Personal Data by Cyren; (iii) ensuring the removal of any and all sensitive Personal Data before any data or requests are submitted to Cyren; and (iv) ensuring that all necessary consents have been obtained from Data Subjects to enable the processing of Personal Data by Subscriber and Cyren (including, but without limitation, in relation to special categories of data).

3. SUBSCRIBER'S INSTRUCTIONS

3.1 Cyren will Process Personal Data only to the extent necessary pursuant to Subscriber's instructions and as set forth in the Main Agreement. This includes the Processing of Personal Data as part of the Services ordered by Subscriber and in order to provide such Services as set forth in the Main Agreement.

Subscriber instructs Cyren to Process Personal Data: (i) where the Processing is necessary for the provision of the Services and in accordance with the Main Agreement; (ii) as part of any Processing initiated by Subscriber or Subscriber's end users in their use of the Services, and; (iii) to comply with Subscriber's other reasonable instructions (i.e. via email or via support requests) to the extent they are consistent with the terms of the Main Agreement and this DPA.

3.2 **Individual instructions.** Subscriber instructs Cyren to Process Personal Data as described in section 3.1 above. Any additional individual instructions must be coordinated between the parties and documented via configuration of the Services through the relevant customer portals or support processes (or as otherwise may be agreed in writing). Cyren shall inform Subscriber immediately if it believes that an instruction violates any Data Protection Laws. In such case, Cyren shall be entitled to defer adherence to such instruction until it is confirmed or changed by Subscriber.

4. TYPES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

4.1 **Types of Data.** The Processing of Personal Data within the scope of this DPA pertains to the following data types/data categories:

- User data (i.e. data submitted as part of the registration process);
- Content data (i.e. content of electronic communications);
- Usage data (i.e. information arising during the use of a Service);
- Communication metadata (i.e. data processed for the purposes of transmitting, distributing or exchanging electronic communications content).

Data may, subject to the particular Services being used, include:

- name, email envelope, email subject;
- User authentication data such as user IDs (i.e. from Subscriber's corporate directory and/or as may be assigned by Cyren);
- Transaction logs;
- IP addresses;
- URLs;
- Phone Numbers;
- Content and connection data;
- Full email including attached files.

4.2 **Categories of Data Subjects.** The group of Data Subjects affected by the Processing of Personal Data within the scope of this DPA includes:

- Subscriber's employees or other authorized users;
- Individuals with whom users correspond via email;
- Third parties whose personal data is contained in the content of the emails to be categorized within the scope of the Services.

5. TERM AND TERMINATION

The term of this DPA, including its Exhibits, corresponds with the term of the Main Agreement. The DPA, (including its Exhibits) and the Processing of Personal Data in accordance with its terms, will terminate simultaneously and automatically with the termination of the Main Agreement.

6. TECHNICAL AND ORGANISATIONAL MEASURES

6.1 Cyren implements and maintains the technical and organizational data protection and data security measures described in **Exhibit 1**.

6.2 The technical and organizational measures are subject to technological progress and advancements. As such, Cyren may implement alternative, adequate measures which meet or exceed the security level of the measures described in **Exhibit 1**. Cyren will document any significant changes.

7. OBLIGATIONS OF CYREN

In addition to its other obligations under this DPA, Cyren will also carry out the following duties:

7.1 **DPO.** Appoint a data protection officer in writing, where applicable or – where legally not required – a privacy expert;

7.2 **Obligation to data secrecy**. Ensure that all employees of Cyren who have access to Personal Data within the scope of this DPA have undertaken to comply with the principle of data secrecy and the telecommunication secrecy, as well as to be obligated to treat the Personal Data as strictly confidential and have been informed (i) of the applicable data protection obligations resulting from this DPA and (ii) of the fact that they are bound to only utilize the Personal Data as per Subscriber's instructions and for the specified purposes;

7.3 **Assistance with Data Subject request.** Follow the requirements specified in Section 8 for assisting Subscriber to respond to requests from Data Subjects;

7.4 **Notification in case of investigations.** Immediately notify, if legally permitted, Subscriber about monitoring activities, investigations and other measures carried out by any data protection supervisory authorities or other authorities (e.g. law enforcement agencies, intelligence services etc.);

7.5 **Monitoring DPA Implementation.** Monitor the proper implementation, fulfillment and execution of this DPA;

7.6 **Verification of TOMs.** Verification of the implementation and maintenance of its technical and organizational measures;

7.7 **Assistance with Data Impact Assessments.** Provide, upon Subscriber's request, Subscriber with reasonable cooperation and assistance needed to fulfill Subscriber's obligation under the GDPR to carry out a data protection impact assessment related to Subscriber's use of the Services, to the extent Subscriber does not otherwise have access to the relevant information, and to the extent such information is available to Cyren. Cyren shall provide reasonable assistance to Subscriber in the cooperation or prior consultation with the supervisory authority in the performance of its tasks described above; and

7.8 **Record of Processing Activities**. Maintain a record of all categories of processing activities carried out on behalf of Subscriber.

8. DATA SUBJECT REQUESTS.

8.1 Cyren shall, to the extent legally permitted, promptly notify Subscriber if Cyren receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request").

8.2 Taking into account the nature of the Processing, Cyren shall assist Subscriber by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Subscriber's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Subscriber, in its use of the Services, does not have the ability to address a Data Subject Request, Cyren shall upon Subscriber's request provide commercially reasonable efforts to assist Subscriber in responding to such Data Subject Request, to the extent Cyren is legally obliged or permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Subscriber shall be responsible for any costs arising from Cyren's provision of such assistance.

9. NOTIFICATION IN THE EVENT OF VIOLATIONS BY CYREN

Cyren shall notify Subscriber without undue delay, after becoming aware of a Personal Data Breach via e-mail to the contacts provided by Subscriber in writing. Such notice shall include a description of the nature of the Personal Data Breach and, where possible, other information as is required by applicable Data Protection Law(s); provided, that, where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

In such cases, Cyren will take all commercially reasonable measures, in consultation with Subscriber, to secure the data and to minimize possible harmful consequences to the Data Subjects affected.

10. SUBCONTRACTING / SUB-PROCESSORS

10.1 **Permitted Use.** Subscriber acknowledges and agrees that (i) Cyren is entitled to retain its affiliates as Sub-Processors, and (ii) Cyren or any such affiliate may engage third parties from time to time to process Personal Data in connection with the provision of Services as Sub-Processors. Cyren will only disclose Personal Data to Sub-Processors that are parties to written agreements with Cyren including obligations no less protective than the obligations of this DPA.

10.2 The Sub-Processors currently engaged by Cyren and authorized by Subscriber are listed at Cyren's Sub-Processor web page (the 'Sub-Processor List") at https://www.cyren.com/legal/sub-processor-list.

10.3 Cyren will provide Subscriber with advance notice before a new Sub-Processor processes any Personal Data. Subscriber may object to the new Sub-Processor within fifteen (15) days of such notice on reasonable grounds relating to the protection of Personal Data by following the instructions set forth in the Sub-Processor List. In such case, Cyren shall have the right to cure the objection through any one of the following options (to be selected at Cyren's sole discretion): (i) Cyren will cancel its plans to use the Sub-Processor with regards to processing Personal Data or will offer an alternative to provide the Services without such Sub-Processor; or (ii) Cyren will take the corrective steps requested by Subscriber in its objection notice (which remove Subscriber's objection(s)) and proceed to use the Sub-Processor; or (iii) Cyren may cease to provide or Subscriber may agree not to use (temporarily or permanently) the particular aspect or feature of the Services that would involve the use of such Sub-Processor. If none of the above options are commercially feasible, in Cyren's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days after Cyren's receipt of Subscriber's objection notice, then either party may terminate the Agreement for cause without a refund of any pre-paid fees. Such termination right is Subscriber's sole and exclusive remedy if Subscriber objects to any new Sub-Processor.

10.4 For the purposes of this section, sub contractual relationships are understood to be those services which are directly related to the provision of the primary service. This does not include ancillary services which Cyren uses, for example, as (tele)communications services, postal/transport services, maintenance and user service or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. Maintenance and testing services shall constitute a sub-processing relationship if they are provided for IT systems which are directly related to the service provided by the Cyren under this Agreement. Cyren shall, however, be obliged to make appropriate and legally binding contractual arrangements including technical and organisational measures and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.

10.5 **Liability**. Cyren shall be liable for the acts and omissions of its Sub-Processors to the same extent Cyren would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

11. DATA TRANSFERS

11.1 With respect to the Services listed in **Exhibit 2**, Cyren shall Process Personal Data only within the territory of the European Economic Area (EEA) or, where support services are being provided, the United Kingdom (UK) on basis of the UK adequacy decision of the European Commission; Subscriber acknowledges and agrees that certain Personal Data may be transferred to the UK for the provision of support services as further described in Exhibit 2. Any transfer of Personal Data to a location outside of the EEA or the UK shall require Subscriber’s prior written consent and may only take place if the specific requirements under applicable Data Protection Laws for a data transfer to the respective Third Country are met.

11.2 With respect to the Services listed in **Exhibit 3**, Cyren shall Process Personal Data only within the territory of the European Economic Area (EEA) unless the specific requirements under applicable Data Protection Laws for a data transfer to the respective Third Country are met namely because (i) an adequacy decision of the European Commission exists, (ii) Standard Contractual Clauses have been implemented, (iii) the data transfer is subject to Binding Corporate Rules, or (iv) other appropriate safeguards have been put in place (each also referred to as "transfer mechanism"). With respect to these Services, Subscriber acknowledges and agrees that certain Personal Data may be transferred to Third Countries. The transfer mechanism Cyren relies on for each transfer to a Third Country is specified in **Exhibit 3**.

11.3 For the avoidance of doubt, Cyren will include obligations no less protective than the obligations of this DPA in the written agreements with Third Country Sub-Processors as provided for in section 10.1 of this DPA. These will apply in addition to any of the Third Country Sub-Processor's obligations as a Data Importer under Standard Contractual Clauses. In the event of a conflict, the provisions of Standard Contractual Clauses shall take precedence over the obligations deriving from this DPA.

12. SUBSCRIBER’S MONITORING RIGHTS

12.1 Subscriber may monitor Cyren’s compliance of its obligations under this DPA. Cyren will ensure that Subscriber has the ability to reasonably assure itself by initiating onsite inspections of Cyren’s adherence to the stipulated technical and organizational measures prior to the commencement of the Processing activities and during the term of this DPA. For this purpose, Cyren will, upon Subscriber's request, provide Subscriber with evidence that the technical and organizational measures described in Exhibit 1 have been implemented.

12.2 Alternatively, Cyren may satisfy its obligations under this section by presenting current attestations, reports, or excerpts of reports from independent authorities (such as accountants, auditors, the data privacy officer, IT security department, data protection auditors or quality auditors) or a suitable certification received within the scope of an IT security or data protection audit (such as pursuant to the German Federal Office for Information Security's "IT-Grundschutz" Certification Program).

12.3 In addition, in the event that Subscriber reasonably believes that the relevant documentation provided by Cyren warrants further examination to demonstrate compliance with Data Protection Laws and this DPA, upon Subscriber's request not less than thirty (30) days in advance, one (1) on-site audit per annual period (except in relation to exceptional incidents or audits required by a supervisory authority under the Data Protection Law) during the Term may be conducted at Cyren facilities involved in the delivery of Services, at reasonable times during business hours and at Cyren's then-current rates. The scope of such audit, including conditions of confidentiality, shall be mutually agreed prior to initiation of the audit.

13. DATA DELETION AND RETURN OF DATA STORAGE DEVICES

After completion of the contractually agreed services (or earlier at Subscriber's request) – at the latest upon termination of the DPA – Cyren shall destroy all Personal Data received or created within the scope of this DPA unless Subscriber provides Cyren with a written requests to transfer the Personal Data at least 4 weeks before termination. Upon request, Cyren shall present the deletion logs to Subscriber.

Documentation materials that serve as evidence that Personal Data was processed in a proper manner consistent with the stipulations of this DPA must be stored by Cyren after termination of this DPA in accordance with the applicable retention periods. Cyren may transfer these documents to Subscriber after termination of the DPA to demonstrate that the Personal Data was processed in a proper manner consistent with the stipulations of this DPA.

14. LIABILITY

14.1 Cyren and Subscriber shall be liable to Data Subjects in accordance with Article 82 of the GDPR.

14.2 Subscriber shall indemnify and hold harmless Cyren from and against any and all claims of third parties (including Data Subjects and data protection authorities) raised against Cyren caused by a breach of Subscriber of any of the provisions of this Agreement and/or Data Protection Laws.

14.3 In no event shall the Cyren's liability to Subscriber in connection with any issue arising out of, or in connection with, this DPA exceed Cyren's limitations on liability set out in the Main Agreement. Cyren's limitations on liability as set out in the Main Agreement shall apply in aggregate across both the Main Agreement and this DPA, such that a single limitation on liability regime shall apply across both the Main Agreement and this DPA.

14.4 Notwithstanding the above, nothing in this DPA shall limit or exclude either party's liability for any liability that cannot be excluded or limited by law.

15. GOVERNING LAW

This DPA shall be governed by the laws of the same jurisdiction as agreed in the Main Agreement.

EXHIBIT 1

Technical and organizational measures (TOM)
within the meaning of Art. 32 DSGVO

Cyren shall ensure the appropriate level of protection pursuant to Article 32 of the EU General Data Protection Regulation (GDPR) for the processing of the data designated in the subject matter of the contract by means of the technical and organizational measures described below.
Unless otherwise described, the information refers to the location Heidestrasse 10, 10557 Berlin, Germany.

The above organization meets this requirement through the following measures:

1. Confidentiality

1.1. Equipment Access control

The following measures have been taken to prevent unauthorized persons from accessing the data processing facilities:

Physical Access

Adequate data center security, access control, and the specification of authorized persons will be used to prevent unauthorized persons from accessing the data processing systems.

Office: An access control system is used to prevent unauthorized access. Visitors are welcomed at the reception and personally guided through the office. Employees use key cards for entering the office.

The internal technical room is secured with a security lock and only a limited number of Service Provider employees (technical administration) have access.

Data Centers: Security personnel and an alarm system is used to prevent unauthorized access to the data center's data processing systems. Access is restricted to authorized persons after presenting photo identification; Processors head of service operation and head of information technology are the only people with permission to determine who is authorized. Data processing systems are locked separately using combination locks, and the combinations are only known by authorized persons.

The external Data Centers in the EU are certified acc. ISO 27001.

1.2. Data media access control - Physical security of the infrastructure

The following measures have been taken to prevent unauthorized persons from gaining access to data processing equipment:

Every Cyren employee has a personal password-protected login name.
The authorization concept is realized via Active Directory group policies.

External access to the workstations is prevented using firewalls and workstations are protected with anti-virus software that updates itself automatically. The use of spam filters and regular control is implemented.

Mobile IT systems (notebooks / iPhones) are encrypted and equipped with Anti-Virus software.

Communication within Cyren as well as between the workstations and the data processing systems in external data centers is carried out exclusively via secure channels (either encrypted or dedicated lines). Dedicated lines or encrypted channels (VPN) exist between Cyren's offices and the data centers as well as between the data centers themselves which third parties cannot access.

External access to the company network (outside sales, employees working from home) is carried out exclusively over an encrypted VPN connection. Access to the VPN is secured using a Multi-Factor Authentication. In addition, separate VPN access is required for establishing VPN connections to Company offices and data center environments.

1.3. Storage control

The following measures have been taken to ensure that the person authorized to use a data processing system can access exclusively the data according to their access authorization level and that personal data cannot be read, copied, modified or deleted during processing, use and after storage by unauthorized persons:

Workstations: Password policy incl. password length, password change is in place. Every Cyren employee has a personal password-protected login name with waiting intervals in the event that an incorrect password is entered in multiple times. Employees are instructed to use secure passwords (sufficiently long combinations of different types of characters, no well-known words or names) and to keep their passwords secret.

Applications: the accesses to applications, specifically when entering, changing, and deleting data are logged.

Role and rights management with differentiated access rights and approval routines are implemented. Within the scope of Cyren's permissions model, access authorization for Cyren employees is restricted in such a way that each employee can only exert influence on the data processing steps necessary for them to complete their work. When leaving the company, the employees will have all access rights revoked.

The number of administrators is limited to what is necessary. Administration rights are graded in system administration and database administration.

Approval routines are in place. Every employee who needs to get access to a system has to get an approval of its manager. This manager must belong to the group of approvers and be authorized to give the approval.

Remote access to productive systems requires the use of the company VPN.

Access to the VPN is logged so that work carried out within the company network from external sales employees and those working from home is traceable.
Before reuse, data media will be deleted or destroyed physically acc. DIN 32757.
Paper document shredding bins are available in the office.
Data media is securely stored in the technical room. Destruction of data media in accordance with a recognized standard (e.g. DIN 32757), Logging of destruction.

1.4. Separation control

The following measures have been taken to ensure that data collected for different purposes can be processed separately:

The affected databases are not connected. Depending on the use case, the separation of data sets is guaranteed through either physical separation when Cyren uses its own servers within a colocation DC or separation at the application level, when Cyrens is using Cloud Services.

Production and test environments are separated and with the Active Directory group policies an authorization concept is realized.

2. Integrity

2.1. Transfer control

The following measures ensure that personal data cannot be read, copied, modified or erased without authorization during electronic transmission or while being transported or stored on data carriers, and that it is possible to verify and determine where personal data can be transmitted to by data transmission equipment:

Data is transmitted exclusively to the recipient or recipients concerned via the respective destination device for the purpose of rendering the contractual services and the subsequent transfer of transmitted data. Encrypted transfer is carried out by default, insofar as Cyren has previously received the data in this way from the Customer.

Technical updates are deployed over encrypted connections (SSL, VPN). The data transmission and data transports are logged.

Cyren employees must dispose of documents and data storage devices containing personal Data securely as soon as they no longer need to be retained.

2.2. Input control

The following measures ensure that it is possible to check and determine retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed:

Within the scope of Cyren’s permissions model, access authorization for Cyren employees is restricted in such a way that each employee can only exert influence on the data processing steps necessary for them to complete their work.

To implement this, Cyren employees are organized into groups based on department and duties, with permissions granted in accordance with the requirements. Group policies are realized in the Active Directory.

Cyren adheres to the principle that permissions are granted at the lowest level necessary to carry out the respective duties. If an employee’s area of activity changes, their assignment to the respective group is also changed, and with it, the corresponding permissions.

Furthermore, Cyren also utilizes the aforementioned firewall systems and user authorization and authentication measures.

Access to the VPN is logged so that work carried out within the company network from external employees and those working from home is traceable.

Traceability of input, modification and deletion of data through individual user names (not user groups) is implemented where applicable.

3. Availability and resilience

3.1. Availability **control**

The following measures ensure that personal data is protected against accidental destruction or loss:

Cyren uses colocation providers (housing) with ISO 27001 certifications to operate its own infrastructures. The infrastructure is redundant. Copies are mirrored in geographically separated DCs. (1 Master-3Salves)

For certain cloud services, Cyren uses third-party infrastructure and services (hosting)

Processed Data: Cyren will always take the necessary measures to ensure that its service has the highest possible level of availability. As a matter of principle, personal Data is processed on redundant systems.

Stored Data: Data stored over longer periods of time is secured through the regular creation of backups. The backup process has two stages: the data is initially stored on hard drives at the data center (for rapid recovery), then on tape (for secure storage). In certain circumstances, the tape backups are encrypted and stored in another building. Data that, due to its size, cannot be stored as a normal backup is permanently saved as multiple copies at different geographical locations.

The data centers protected against emergencies using advanced technology.

Cloud Service Providers: For its Cloud Services Cyren uses a Cloud Service Provider, that is instructed to store the data within the EU region.

Operational readiness by our own team exists 24 hours a day. Security concept for software and IT applications exist

3.2 Timely restoration

The following measures ensure that in the event of a physical or technical incident, the availability of and access to personal data is restored in a timely manner:

See also 3.1.

Office: A security concept for software and IT applications is in place.

Operational Data: All processing systems are built redundant and can be restored in a timely manner. Only in rare cases Cyrens stores personal data of its customers at all, e.g. for configuration settings.

4. Effectiveness controls - Procedures for periodic review, assessment, and evaluation

4.1. Data protection management

The following measures ensure that the Contractor's data protection and information security organization is designed in such a way that it meets the requirements of the described commissioned processing and the general legal requirements:

- Cyren GmbH has appointed an internal Data Protection Officer.
- Cyren uses a software solution for data protection management.
- The employees are trained and bound to confidentiality/data secrecy agreements.
- A formalized process for processing requests for information from data subjects is in place.
- A data protection impact assessment (DPIA) can be carried out if applicable.
- Cyren complies with the information obligations according to Art. 13 and 14 GDPR.
- Directory of processing activities acc. Art. 30 Section 2 GDPR are documented.
- An Incident management system incl. process for handling data breaches is handled by an incident management team.

- There is a procedure for handling inquiries from data subjects, and the departments involved are trained to deal with such inquiries.

4.2. Incident management

The use of firewall, spam filter and virus scanner are mandatory for all users, who don't work with malicious material. They are regularly updated.

An incident management team is in place. Security incidents are documented. A formal Root Cause Analysis (RCA) procedure is applied to relevant security incidents.

Security incidents and data breaches are documented and there is a documented procedure for handling security incidents and data breaches.

The data protection officer and the privacy team will be informed about security incidents that might cause data breaches.

4.3. Privacy by design / Privacy by default

The following measures ensure that, by default, only personal data whose processing is necessary for the respective specific processing purpose are processed:

Cyren GmbH follows a privacy by design approach and "builds in" by code specific measures for pseudonymization and deletion/overwriting of data.

Cyren does not collect more personal data than is necessary to achieve the respective purpose and processes the personal data only for as long as it is necessary to fulfill the respective purpose.

Parameters were coded to reject data that is no longer needed.

Automated overwriting routines of the processing systems are implemented, routines after the end of processing or after the purpose of processing no longer applies.

The relevant personnel, especially from the detection and engineering teams, are trained in particular with regard to data protection.

Personal Data is usually managed by the Customer itself or transmitted to Cyren by the Customer.

4.4. Processing control (outsourcing to third parties)

The following measures ensure that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions. This section also includes the performance of maintenance and system support work both on site and via remote maintenance. If the Contractor uses service providers in the sense of processing of personal data according to Art 28 GDPR, the following points must always be regulated with them:

Cyren only discloses Personal Data to Sub-processors that are parties to applicable written agreements with Cyren including obligations no less protective than the obligations of this DPA. This includes to agree on effective control rights vis-à-vis the processor as well as the obligation of the processor's employees to maintain data secrecy.

EXHIBIT 2

Processing within EEA and UK territory only: Processing of Personal Data only within the territory of the European Economic Area (EEA) or the United Kingdom (UK), including account management and technical support services as described in the Cyren Support Services datasheet posted at www.cyren.com/legal .

Product	Location of Services	Location of Support Services	UK Transfer Mechanism	UK Processor or Sub-Processor
Cyren Email Security (my.Eleven - Single Engine)	Germany	UK	Adequacy decision	Cyren UK Ltd.
Cyren DNS Security	Germany	UK	Adequacy decision	Cyren UK Ltd.
Cyren Cloud Sandboxing (EU Region)	Germany	UK	Adequacy decision	Cyren UK Ltd.
Cloud Threat Lookup (EU Region)	Germany	UK	Adequacy decision	Cyren UK Ltd.
CES Inhouse	Germany	UK	Adequacy decision	Cyren UK Ltd.

EXHIBIT 3

A. With respect to the products listed in the table below, Personal Data is transferred to and/or accessed from outside of the EEA only if Tier 3 or Tier 4 support or maintenance services are provided to the Customer as set forth in the table below.

Product	Location	Transfer Mechanism	Processor or Sub-Processor
Cyren Cloud Security - Email (Single Engine)	Israel/ UK	Adequacy decision	Cyren Ltd./ Cyren UK Ltd.
Cyren Email Archiving	Israel/ UK	Adequacy decision	Cyren Ltd./ Cyren UK Ltd.
Cyren Inbox Security	Israel/ UK	Adequacy decision	Cyren Ltd./ Cyren UK Ltd.

B. With respect to the products listed in the table below, Personal Data is also transferred to and/or accessed from outside of the EEA as set forth in the table below.

Product	Location	Transfer Mechanism	Processor or Sub-processor
Cyren Cloud Security - Email (Dual Engine)	Israel/ UK United States	Adequacy decision Standard Contractual Clauses[1]	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Cyren Email Security (my.Eleven - Dual Engine)	Israel/ UK United States	Adequacy decision Standard Contractual Clauses	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Cyren Cloud Sandboxing (US Region)	Israel/ UK United States	Adequacy decision Standard Contractual Clauses	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Cloud Threat Lookup (US Region)	Israel/ UK United States	Adequacy decision Standard Contractual Clauses	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Incident Response Service for Cyren Inbox Security	Ukraine	Standard Contractual Clauses	Cyren. Ltd.

[1] EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021