DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is incorporated into the Subscription Agreement and all related orders directly between Subscriber and Cyren and reflects the parties' consent with regard to the Processing of Personal Data. This DPA consists of the main body of the DPA and Exhibits 1, 2 and 3.

HOW TO EXECUTE THIS DPA

1. This DPA has been pre-signed on behalf of Cyren.
2. To complete this DPA and make it part of the Subscription Agreement, Subscriber must complete the information in the signature box of this DPA and have an authorized representative sign on page 7.
3. Send the completed and signed DPA by email to dpa@cyren.com. Please also include a copy of your order form and/or Subscription Agreement with Cyren.

Upon receipt of the completed and signed DPA by Cyren, this DPA will become valid and legally binding. This DPA will not become valid and legally binding if the signing Subscriber is not a party to the Subscription Agreement.

If the Subscriber is not a party to an order or Subscription Agreement directly with Cyren, but is instead a subscriber indirectly via an authorized reseller or other partner of Cyren (regardless of whether Cyren provides support and maintenance directly to Subscriber), this DPA is not applicable to you. Contact the entity with whom you have a direct agreement or contact Cyren via privacy@cyren.com for assistance.

DATA PROCESSING TERMS

1. DEFINITIONS

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

"**Cyren**" means (i) Cyren GmbH which has its registered address at Hardenbergplatz 2, 10623 Berlin, Germany, or (ii) if an Order has been placed, the Cyren entity with whom an Order has been placed.

"**Data Controller**" means the entity that determines the purpose and means of the Processing of Personal Data.

"**Data Processor**" means the person which processes Personal Data on behalf of the Data Controller".

"**Data Subject**" means an identified or identifiable natural person to whom the Personal Data relates.

"DPA" means this Data Processing Agreement.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Subscription Agreement.

"**Personal Data**" means any information relating to a Data Subject.

"**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automatic means, such as collection,

recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Services**" has the same meaning ascribed to it in the Subscription Agreement.

"Subscriber" means the party to the Subscription Agreement.

"**Subscription Agreement**" means the Cyren End User Subscription Agreement – Europe (or other sales agreement if applicable) including all related orders entered into between Cyren and Subscriber.

2. PROCESSING OF PERSONAL DATA

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 **Cyren's Processing or Personal Data.** Cyren will Process Personal Data only to the extent necessary pursuant to Subscriber's instructions and as set forth in the Subscription 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 Subscription 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 Subscription 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 Subscription Agreement and this DPA.

2.3 **Compliance with Data Protection Laws.** Subscriber's submission of Personal Data to Cyren and instructions for the Processing of Personal Data will comply with Data Protection Laws.

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

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

- ☐ Full name, email envelope;
- ☐ 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;
- ☐ Content and connection data;
- ☐ Full email including attached files (with respect to Cyren Archiving Service and Quarantine only).

2.5 **Affected Group.** 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 Subscriber's employees 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.

3. TERM AND TERMINATION

The term of this DPA, including its Exhibits, corresponds with the term of the Subscription Agreement. The DPA, including its Exhibits, will terminate simultaneously and automatically with the termination of the Subscription Agreement.

4. TECHNICAL AND ORGANISATIONAL MEASURES

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

4.2 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.

5. ACCESSING, CORRECTION, BLOCKING AND DELETION OF PERSONAL DATA

5.1 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"). 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 fulfilment 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 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.

6. CONTROL OBLIGATIONS AND OTHER DUTIES OF CYREN

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

- ☐ Appoint a data protection officer in writing;
- ☐ 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, are 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 the Subscriber's instructions and for the specified purposes.
- ☐ Immediately notify the Subscriber about monitoring activities, investigations and other measures carried out by any data protection supervisory authorities;
- ☐ Monitor the proper implementation, fulfillment and execution of this DPA by means of regular inspections carried out by Cyren;

- ☐ Ensure that the Subscriber can verify the implementation and maintenance of the technical and organizational measures. This can be done by Cyren submitting (i) current attestations, reports, or excerpts of reports from independent authorities (such as accountants, auditors, data privacy officers, IT security department, data protection auditors or quality auditors) or (ii) 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).
- ☐ Upon Subscriber's request, Cyren shall provide the Subscriber with reasonable cooperation and assistance needed to fulfil Subscriber's obligation under Regulation (EU) 2016/679 ("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 the Subscriber in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks described above.

7. SUBCONTRACTING

7.1 **Appointment of Sub-processors**. 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 any third parties from time to time to process Personal Data in connection with the provision of Services. 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. Cyren will, following the Subscriber's written request, provide to the Subscriber the names of its Sub-processors processing the Personal Data and the countries in which such data is or may be processed.

7.2 **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,

7.3 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 www.cyren.com/legal/sub-processor-list.

7.4 Cyren will provide Subscriber with advance notice before a new Sub-processor processes any Personal Data. Customer 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 products 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 (3) Cyren may cease to provide or Subscriber may agree not to use (temporarily or permanently) the particular aspect or feature of the product 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.

8. DATA TRANSFERS

With respect the services listed in Exhibit 2, Cyren shall Process Personal Data only within the territory of the European Economic Area (EEA). Any transfer of Personal Data to a location outside of the EEA shall require the Subscriber's prior written consent and may only take place if the specific requirements under applicable Data Protection Laws for a data transfer to a country outside the EEA are met.

With respect 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 a country outside the European Economic Area are met. With respect to these services, Subscriber acknowledges and agrees that certain Personal Data may be transferred to Cyren Ltd. in Israel or Cyren Inc. in the United States. Cyren Inc., has certified to the EU-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, in order to ensure an adequate level of protection for the transferred Personal Data pursuant to Article 45 of the GDPR. In the event that the EU-U.S. Privacy Shield Framework is ever deemed invalid, the parties agree to negotiate in a timely way and in good faith any replacement terms as may be required for the international transfer of such Personal Data.

9. SUBSCRIBER'S MONITORING RIGHTS

The Subscriber may monitor Cyren's compliance of its obligations under this DPA by itself or, in individual cases, by an auditor of its choice. Cyren will ensure that the Subscriber has the ability to reasonably assure itself 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 the Subscriber's request, provide the Subscriber with evidence that the technical and organizational measures described in **Exhibit 1** have been implemented.

Alternatively, Cyren may satisfy its obligations under this section by presenting a current attestation, 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).

10. NOTIFICATION IN THE EVENT OF VIOLATIONS BY CYREN

Cyren shall notify the Subscriber in all cases of violations by Cyren or its employees of provisions to protect the Subscriber's Personal Data or in cases of violations of the terms of this DPA.

Cyren shall notify the Subscriber immediately of any loss or unlawful transfer of Personal Data or when third parties gain access to the Personal Data. This also applies in the event of severe disruptions to business operations, in the event of suspicion of other violations of Data Protection Laws, or other irregularities in the handling of the Subscriber's Personal Data. In such cases, Cyren will be obligated to undertake suitable measures, in consultation with the Subscriber, to secure the data and to minimize possible harmful consequences to the Data Subjects affected.

11. SUBSCRIBER'S INSTRUCTIONS

The Subscriber instructs Cyren to Process Personal Data as described in section 2.2 above. The parties agree that this DPA supersedes any prior data processing agreements (including any prior ADV). Any additional instructions must be coordinated between the parties and documented. Cyren shall inform the 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 the Subscriber.

12. DATA DELETION AND RETURN OF DATA STORAGE DEVICES

After completion of the contractually agreed services (or earlier at the Subscriber's request) – at the latest upon termination of the DPA – Cyren shall transfer to the Subscriber all Personal Data received or created within the scope of this DPA or destroy the Personal Data in accordance with applicable Data Protection Laws. Upon request, Cyren shall present the deletion logs to the 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 the 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.

13. GOVERNING LAW

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

ACCEPTED AND AGREED TO:

Subscriber

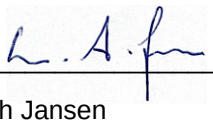
Signature _____

Print Name: _____

Title: _____

Date:_____

Cyren GmbH

Signature 

Name: Ulrich Jansen

Title: Managing Director

Date: May 15, 2018

Cyren UK Ltd.

Signature 

Name: Atif Ahmed

Title: VP, EMEA

Date: May 15, 2018

Cyren Ltd.

Signature 

Name: Eric Spindel

Title: General Counsel

Date: May 15, 2018

EXHIBIT 1

Technical and Organizational Measures

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.

The internal data center is secured with a security lock and only a limited number of Cyren 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; Cyren's 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.

Data Access

Data processing systems cannot be used by unauthorized persons. In order to guarantee this, the following measures have been taken: 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. Passwords must be changed regularly. 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.

External access to the workstations is prevented using firewalls and workstations are protected with anti-virus software that updates itself automatically.

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 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.

Data Usage

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. 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.

Pseudonymization

Cyren has implemented adequate measures for the pseudonymization of certain Personal Data, i.e. the substitution of the data's personal identifiers with non-personal information. The attribution key which allows Cyren to re-connect the pseudonymized data with the relevant Data Subject will be processed separately and secured.

Encryption

Cyren uses encrypting technologies (algorithms, etc.) to ensure that certain Personal Data processed by Cyren is stored, recorded and transferred in an unrecognizable (encrypted) format.

Transfer

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 can be carried out at the request of the Subscriber as an additional service, insofar as Cyren previously received the data from the Subscriber in such a manner.

The use of USB flash drives, portable hard drives, and other portable data storage devices at Cyren's workstations is prohibited as set forth in Cyren's guidelines for using IT resources.

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

Data Entry

Personal Data is usually managed by the Subscriber itself or transmitted to Cyren from the Subscriber or third parties. Alteration, deletion, or data entry by Cyren is only carried out in special cases at the explicit demand of the Subscriber, insofar as technically possible.

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.

Availability

Cyren will take the necessary measures at all times to ensure that its service has the highest possible level of availability. As a matter of principle, Personal Data is processed on redundant systems. 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 that process data are protected against emergencies using advanced technology.

Resilience

Cyren is regularly patching, updating and hardening its data processing systems in order to ensure that they are kept on a state-of-the-art of technology level. This is accomplished in particular by: (i) appropriately testing and applying software patches and upgrades on a regular basis;(ii) risk assessments to identify security vulnerabilities and application of patches to vulnerabilities posing significant risks as soon as possible;(iii) application of relevant patches to known security vulnerabilities; and (iv) established security incident management procedures to address security incidents.

Separation

The unauthorized combining of data outside of its defined purpose is impossible due to the technical design of the processes Cyren uses (the affected databases are not connected). Depending on the use case, the separation of data sets is guaranteed through either physical separation or separation at the application level.

EXHIBIT 2

Cyren Email Security (my.Eleven - Single Engine)

Cyren DNS Security

Cyren Cloud Sandboxing (EU Region)

Cloud Threat Lookup (EU Region)

CES Inhouse

EXHIBIT 3

A. With respect to the products listed in the table below, all Personal Data is stored in EEA-based data centers. Certain support services are performed outside of the EEA (which involve the Processing of Personal Data) as set forth in the table below.

Product	**Services performed outside EEA**	**Location**	**Legal Basis of Transfer**	**Data Importer**
Cyren Cloud Security - Email (Single Engine)	Tier 3 and Tier 4 Support	Israel	Adequacy decision	Cyren Ltd., Israel
Cyren Email Archiving	Tier 3 and Tier 4 Support	Israel	Adequacy decision	Cyren Ltd., Israel
Cyren Cloud Security - Web (EU Region)*	Tier 3 and Tier 4 Support	Israel	Adequacy decision	Cyren Ltd., Israel

*As of June 21, 2018

B. With respect to the products listed in the table below, Personal Data is processed outside of the EEA as set forth in the table below.

Product	**Location**	**Legal Basis of Transfer**	**Data Importer**
Cyren Cloud Security - Email (Dual Engine)	Israel United States	Adequacy decision EU-U.S. Privacy Shield	Cyren Ltd., Israel Cyren Inc., USA
Cyren Email Security (my.Eleven - Dual Engine)	Israel United States	Adequacy decision EU-U.S. Privacy Shield	Cyren Ltd., Israel Cyren Inc., USA
Cyren Cloud Security - Web (US Region)	Israel United States	Adequate decision EU-U.S. Privacy Shield	Cyren Ltd., Israel Cyren Inc., USA
Cyren Cloud Sandboxing (US Region)	Israel United States	Adequate decision EU-U.S. Privacy Shield	Cyren Ltd., Israel Cyren Inc., USA
Cloud Threat Lookup (US Region)	Israel United States	Adequate decision EU-U.S. Privacy Shield	Cyren Ltd., Israel Cyren Inc., USA