DRAFT

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

J2 Global Denmark A/S (Vipre Security Group)
CVR 28117833
Spotorno Alle 12
2630 Tåstrup, Høje Taastrup
Denmark
(the data processor)

and

AX VI itm8 Holding ApS
CVR 42520292
Dalgas Plads 7B
7400 Herning

(the data controller)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses), in accordance with the "Standard Contractual Clauses" issued by the Danish Supervisory Authority as adopted by the European Data Protection Board on July 19th 2019 including same structure and indexing, in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of E-mail Security, Scanning and storage of E-mails, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 36hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet in Denmark, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities,

with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data processor

Name	Robert den Drijver
Position	VP EMEA B2B & Global head of B2B2C
Date	5/10/2023
Signature	DocuSigned by: Robert den Drijver EA835E89545A46A...

On behalf of the data controller

Name	Mikael Kjærgaard
Position	CFO, Group finance
Date	25-03-2023
Signature	Mikael Kjærgaard

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   On behalf of the data controller

Name	Compliance & Security
Telephone	+45 7026 2988
E-mail	compliance@itm8.com

   On behalf of the data processor

Name	Legal Department
Position	Legal Counsel
Telephone	+353861958335
E-mail	legal@ziffdavis.com

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The main purpose is to carry out the Services as set out by the relevant agreement between the parties. This involves to following processing of personal data:

- The scanning of incoming e-mails to determine if the e-mails are affected by virus, spam or phishing-attempts
- Block dangerous attachments – the system checks attachments in the "Sandbox enviroment"
- Ensure that e-mails are sent and received securely and by the use of Tunnel, securemail, TLS, secure mail portal
- Backup of all incoming and outgoing e-mails for a maximum of 90 daysAll correspondence from public authorities is received through Vipre as dictated by the Domain name servers(DNS) Mail Exchange(MX) Records.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

- Scanning and encryption of e-mails
- Storage/backup of e-mails

A.3. The processing includes the following types of personal data about data subjects:

The processing will relate to user-generated content in the form of data controller received and sent e-mails,. Therefore, the processing can potentially include all types of personal data, including ordinary personal data, social security numbers, criminal records, and sensitive personal data.

A.4. Processing includes the following categories of data subject:

The processing can potentially include all types of data subjects, including the controller's customers, suppliers, employees, persons associated with the controller's employees and other staff and persons affiliated with such staff groups.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The Clauses enter into force on the date of signing and are valid as long as the data processor or its possible sub-data processors process personal data on behalf of the data controller or until the termination of the Clauses in accordance with the rules in the Clauses, whichever comes later.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME/ADDRESS	COMPANY NUMBER	LOCATION OF PROCESSING	DESCRIPTION OF PROCESSING
Amazon Web Services		Each datacentre is backed up to a different AWS instance as follows: VIPRE Datacenter: Sweden AWS location: Sweden VIPRE Datacenter: Denmark AWS location: Germany VIPRE Datacenter: Ireland AWS location: Ireland VIPRE Datacenter: UK AWS location: UK	System Backups for each datacentre– emails, meta data/logs, data contained in each datacentre SMS Alert Service – contact details for alerts Data is encrypted with AES-256-CBC and encryption keys are held by VIPRE.
ThreatTrack Security, Inc. at 311 Park Place Boulevard, Suite 300, Clearwater, FL, 33759-3994		United States	To analyse data to improve the spam filtering services provided by VIPRE This is not automatic, customer must give their active consent Metadata and email content of false positive and false negatives submitted for review by customers.
ThreatTrack Security, Philippines, Inc 5th Floor One World Square Building, Upper Mckinley Road, Brgy. Pinagsama, Fort Bonifacio, Taguig City,		Philippines	To analyse data to improve the spam filtering services provided by VIPRE This is not automatic, customer must give their active consent. Metadata and email content of false positive and false negatives submitted for review by customers
Terro Green Ltd. Bulgaria, Sofia, Lozenets, Plachkovica 2 street. Post code 1407	BG201235010	EEU	– Monitor malware and spam detection accuracy and performance -Investigate false positives and false negatives-

NAME/ADDRESS	COMPANY NUMBER	LOCATION OF PROCESSING	DESCRIPTION OF PROCESSING
			Create new rules to detect missed malware -Analyse detected malware to identify emerging trends and threats
Google Compute Cloud Germany		EEU	The Scanning of email attachments for the purpose of protection against malicious files and carry out behaviour analysis. Once the processing is completed, the file will be deleted from this system

The list of sub-processors used at the time of contracting is inserted in the above table and will be adjusted in case of acquisition or changes in services.

After commencement of the Clauses, the data processor can use other sub-processors. The data controller will be informed of changes in data processors used upon purchase of new services or data processor changes to services. In addition, an appendix of currently used sub-processors can be provided upon request.

The procedure for the data processor's notice regarding planned changes in terms of addition or replacement of sub-processors is described in clause B.2.

B2. Notice for approval of sub-processors

The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than thirty (30) days before the addition or replacement is to take effect, in so far this is possible.

If the data controller has any objections to such changes, the data controller shall notify the data processor thereof before such change is to take effect. The data controller shall only object to such changes if the data controller has reasonable and specific grounds for such refusal.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed Services. Such non-performance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such services, regardless if they cannot be provided to the data controller.

If it has been specifically agreed that the data processor cannot use sub-processors without the data controller's prior approval, the data controller accepts that this may mean that the data processor may be prevented from providing Services. If the data controller has refused any changes in terms of addition or replacement of sub-processors, non-provision of Services will not be considered a breach of the parties' Service Agreement that can be ascribed to the data processor in situations where not-performance may be ascribed to matters relating to a sub-processor.

B.2. Prior notice for the authorisation of sub-processors

If the data controller:

a. Does not respond (in writing) within 30 days from the date of the notification, it will be deemed to have given its authorisation to the use of such sub-processor; or

b. Responds by refusing (in writing) its authorisation and a mutually acceptable resolution of such refusal cannot be agreed, it may terminate the service or that part of the service provided by the data processor using the relevant sub-processor. This termination right is the data-controller's sole and exclusive remedy if the data controller objects to any new third-party sub-processor.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Enterprise mail scanning and encryption with all security measures as expected for such performance, including backup hosting of e-mails.

C.2. Security of processing

The level of security shall take into account:

The Data Processor shall – 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 – however, the Data Processor shall in all instances subject to GDPR article 32 perform its own risk assessment and implement appropriate security measures for its own account):

The processor declares to follow the requirements in ISAE 3000 and ISAE 3402.

Regarding requirements Regarding pseudonymisation and encryption of personal data: Data Processor refers to its ISAE 3402-1 §10

Regarding requirements for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services: Data Processor refers to its ISAE 3402-1 § 6 and ISAE 3000 pp4-11

Regarding requirements for the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident: Data Processor refers to its ISAE 3402-1 §12 and §16 and §17

Regarding requirements for processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing: Data Processor refers to its ISAE 3402-1 §12 and ISAE 3000 pp 4-11

Regarding requirements for access to data online: Data Processor refers to its ISAE 3402-1 § 9

Regarding requirements for the protection of data during transmission: Encryption by certificate og TLS 1.2 as a minimum is being used.

Regarding requirements for the protection of data during storage:-Data Processor refers to its ISAE 3402-1 § 10 and § 8

Regarding requirements for physical security of locations at which personal data are processed:-Data Processor refers to its ISAE 3402-1 §11

Regarding requirements for the use of home/remote working: Data Processor refers to its ISAE 3402-1 § 6.2

Regarding requirements for logging:-Data Processor refers to its ISAE 3402-1 § 9 and § 12.4 For all the above items, in general, Data Processor refers Vipre/Fusemails latest Audit Statements ISAE 3402 and ISAE 3000, where all relevant processes and procedures are described.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

In accordance with the provisions of 9.1, the data processor shall provide reasonable assistance to the data controller without undue delay, considering the nature and functionality of the service with regard to the data controller's or its customers' obligations regarding:

a. Requests from data subjects for access to or correction, deletion, restriction, blocking or deletion of the data controller's personal data, provided that the data controller acknowledges that when the functionality of the service allows it, such actions must be performed by the data controller.

The data processor is not entitled to respond to requests from a data subject regarding exercising his/her rights under applicable GDPR. If the data processor receives a request from a data subject, such request must, without undue delay, be forwarded to the data controller.

In accordance with the provisions of 9.2, the data processor shall, without undue delay, after becoming aware, and no later than 36hours after becoming aware, of a security breach, notify the data controller in writing of any suspicion or breach of personal data security. The data processor's notification shall include at least the following:

a. A description of the nature of the breach of personal data security, including, if possible, the categories and number of data subjects concerned, as well as the categories and number of personal data records concerned;
b. A description of the likely consequences of the breach of personal data security; and
c. A description of the measures that the data processor has taken or proposes to take to deal with the breach of personal data security, including if applicable, measures to limit its possible harmful effects. If a breach of personal data security occurs at a sub-data processor, the data processor must ensure that the sub-data processor provides the same information as listed above.

The data processor may not communicate publicly or to third parties about security breaches or non-compliance with the data processor agreement without prior written agreement with the data controller on the content of such communication unless that data processor is obliged to such communication by law.

If the data controller assesses that the processing is likely to involve a high risk to the data subjects' rights and freedoms, the data processor shall, at the request of the data controller, assist the data controller in connection with its obligations under Articles 35 and 36 of GDPR by providing the data controller with the information necessary for the data controller to carry out an impact assessment in accordance with Article 35 and to carry out a prior consultation of the Data Protection Agency in accordance with Article 36.

Finally, the data processor must ensure that its technical and organizational measures enable the data controller to comply with his obligations under the nature of the Data Protection Regulation. 33-36, including e.g., through measures concerning management of security breaches, management of assets, logging, etc.

C.4. Storage period/erasure procedures

Storage of e-mails for no more than 90 days unless requested otherwise by the data controller.

Administration and log data are deleted manually no later than 90 days after the termination of the agreement unless otherwise agreed.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the agreement – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

The processing of personal data takes place at the addresses of the data processor as well as the listed data processors and their sub-processors. In addition, remote work may be performed in accordance with the data processor's remote work policy.

C.6. Instruction on the transfer of personal data to third countries

The data controller has authorised and thereby instructed the data processor to transfer personal data to a third country as further specified below. In addition, by subsequent written notification or agreement the data controller can provide instructions or specific consent pertaining to the transfer of personal data to a third country.

If the data controller does not in the Clauses or subsequently provides documented instructions pretraining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer

C.6.1 General approval of transfer of personal data to secure third countries
With these Clauses, the data controller provides a general and prior approval (instructions) for the data processor to transfer personal data to third countries if the European Commission has laid down that the third country/the relevant area/the relevant sector has a sufficient level of protection.

C.6.2 Approval of transfer to specific recipients of personal data in third countries when the necessary guarantees have been provided
The data controller shall instruct the data processor to use the following sub-processor(s) where transfers of personal data to third countries take place:

Name	Company Number	Description of processing	Transfer to a third country
Amazon Web Services		System Backups for each datacentre– emails, meta data/logs, data contained in each datacentre SMS Alert Service – contact details for alerts Data is encrypted with AES-256-CBC and encryption keys are held by VIPRE.	Yes Legal basis: SCC Data is placed inside the EEU, however, support can be performed from outside the EEU. Amazon is subject to American FISA and cloud act warrants and can be forced to transfer data to US law enforcement.
ThreatTrack Security, Inc		To analyse data to improve the spam filtering services provided by VIPRE This is not automatic, customer must give their active consent Metadata and email content of false positive and false negatives submitted for review by customers.	Yes Legal basis: SCC ThreatTrack Security, Inc is subject to American FISA and cloud act warrants and can be forced to transfer data to US law enforcement.
ThreatTrack Security, Philippines, Inc		To analyse data to improve the spam filtering services provided by VIPRE This is not automatic, customer must give their active consent. Metadata and email content of false positive and false negatives submitted for review by customers	Yes Legal basis: SCC
Google Compute Cloud		The Scanning of email attachments for the purpose of protection against malicious files and carry out behaviour analysis. Once the processing is completed, the file will be deleted from this system.	Data is placed inside the EEU, however, support can be performed from outside the EEU. Google Compute Cloud is subject to American FISA and cloud act warrants and can be forced to transfer data to US law enforcement.

When entering into the Clauses, the data controller has given consent to the use of the above sub-processor(s) and instructed on the transfer of personal data to third countries for the provision of the Services.

If the European Commission's Standard Contractual Clauses ("SCC") for the transfer of personal data to a third country are used as the transfer basis, the data processor and/or any sub-processor shall be entitled to enter into such SCCs with the relevant sub-processor.

In the event that the European Commission prepares new SCCs after the conclusion of the Service Agreement, the data processor is authorised to replace, update and apply the SCCs in force at any time.

The contents of this instruction and/or the Clauses shall not be deemed to modify the contents of the SCCs.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall yearly at the data processor's expense, obtain an auditor's report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the clauses:

- ISAE 3000 type 2
  and
- ISAE 3402 type 2 or equivalent from the used datacentres.

On request, the auditor's report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may, in such cases, request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the data controller deems it required.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall yearly at the data processor's expense obtain an auditor's report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses:

ISAE 3000 type 2 or ISAE 3402 type 2 or equivalent.

On request, the auditor's report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall, in addition, have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the data processor (or the data controller) deems it required.

Documentation for such inspections shall, without delay, be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

The data processors and the sub-processor's costs related to physical supervision/inspection at the sub-processor's facilities shall not concern the data controller – irrespective of whether the data controller has initiated and participated in such inspection.

Appendix D The parties' terms of agreement on other subjects

Any dispute or claim arising out of or in connection with the Clauses shall be settled at the Courts and be governed by the laws set out in the agreement between the parties.