EUROPEAN COMMISSION

Brussels, **6.27.2021**

C(2021) 3972 final ANNEX

STANDARD CONTRACTUAL CLAUSES

Unless Customer informs McAfee and requires specific modifications to the below, the following Standard Contractual Clauses, including its exhibits, will be deemed executed between the parties.

(i) SECTION I

(ii) Clause 1 Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

b. The Parties:

  i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

  ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(iii) Clause 2 Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

(iv) Clause 3 Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

(v) Clause 4 Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

(vi) Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

(vii) Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

(viii) Clause 7 – Optional Docking clause

(*omitted*)

(b) SECTION II – OBLIGATIONS OF THE PARTIES

(i) Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

(ii) Clause 9 Use of sub-processors

a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [**Specify time period**] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c. The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.
e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

(iii) **Clause 10 Data subject rights**

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

(iv) **Clause 11 Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   ii. refer the dispute to the competent courts within the meaning of Clause 18.
d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

(v) **Clause 12 Liability**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

(vi) Clause 13 Supervision

a. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

(c)

(d) <u>SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES</u>

(i) Clause 14 Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation

- . The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by
- the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

(ii) Clause 15 Obligations of the data importer in case of access by public authorities

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

(e)

(f) <u>**SECTION IV – FINAL PROVISIONS**</u>

(i) Clause 16 Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   ii. the data importer is in substantial or persistent breach of these Clauses; or
   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

- In these cases, it shall inform the competent supervisory authority

- of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

(ii) **Clause 17 Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

(iii) **Clause 18 Choice of forum and jurisdiction**

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of Ireland.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEXES TO THE SCCs (MODULE 2: CONTROLLER TO PROCESSOR)

ANNEX 1 TO THE SCCs - DESCRIPTION OF THE TRANSFERS

This Appendix forms part of the Transfer Clauses and must be completed and signed by the Parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

I A - DESCRIPTION OF THE PARTIES

Data exporter

The Data Exporter is (i) the company that has executed the Standard Contractual Clauses as a Data Exporter and (ii) all Customer's Affiliates (as defined under the Agreement) established within the European Economic Area (EEA) and Switzerland that export Personal Data under the Agreement. The Data exporter acts as a Processor.

Data importer

The Data Importer is McAfee LLC on behalf of McAfee Ireland Limited and all other McAfee Affiliates. The Data Importer provides Products and Services to the Data Exporter in relation to security products and services under the Agreement between the Data Exporter and the Data Importer, in the course of which it processes certain personal data as a processor. The Data Importer acts as a Controller.

I B - PROCESSING OPERATIONS

Processing operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify):

☐ The Personal Data will be used to provide human resources benefits.

X The Personal Data will be used to provide information technology services to the Customer employees.

X The Personal Data will be used to provide security and data protection Products and Services.

X The Personal Data will be used to enhance McAfee's threat defences.

X The Personal Data will be used to provide Customer with Products and Services.

X The Personal Data will be used to provide licenses to McAfee Products and Services.

On behalf of the data importer:

Name (written out in full): Noémie Weinbaum

Position: Corporate & Privacy Attorney

Address: McAfee, LLC

6220 America Center Drive San Jose, CA 95002. USA

Signature:

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Signature:

ANNEX 2 TO THE SCCs: DESCRIPTION OF THE TRANSFERS

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

☐ Current, former, prospective employees.

☐ Current, former, prospective employees and their dependents.

X Employees of Corporate customers

☐ McAfee consumer customers and former consumer customers

X McAfee Sub-processor's contacts

Categories of data

The Personal Data transferred concern the following categories of data (please specify):

☐ Employees' names and contact information, including home addresses, emails, phone numbers, IP addresses, employment history, education/qualifications, transaction history.

☐ Employees' names and contact information, including addresses, emails, phone numbers, IP addresses; employees' dependents' names and contact information, including addresses, emails, phone numbers.

X McAfee Corporate customers' employees' names and business contact information, including addresses, emails, phone numbers, IP addresses.

☐ McAfee Consumer customers' names and business contact information, including addresses, emails, phone numbers, IP addresses.

X McAfee Sub-processors' contacts, including employees' names and business contact information, including addresses, emails, phone numbers, IP addresses.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

X None.

☐ If you are using / transferring any information about children or an individual's racial/ethnic origin; health; sexuality; political opinions; religious beliefs; criminal background or alleged offences; or trade union membership, this should be noted here.

Please elaborate:

Frequency of the transfer: (the frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). Please tick as applicable.

☐ None.

☐ One-off.

X On-going.

☐ In accordance with the specifications described under the Agreement.

Period of retention: please provide the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

X☐ Limited to the term of the Agreement.

☐ Other. Unless under Legal Hold

☐ criteria used to determine that period. Please specify : Duration of the Legal Hold

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

- Subject matter: please refer to the list of subprocessors
- Nature: please refer to the list of subprocessors
- Duration: for the term of the Agreement

Competent supervisory authority:

☐ Data Protection Commission of Ireland

☐ Other. Please specify: _____________

ANNEX 3
Technical and Organisational Security Measures

This Appendix 2 forms part of the Transfer Clauses and summarizes the technical, organisational and physical security measures implemented by the parties in accordance with Clauses 4(d) and 5(c).

McAfee have implemented technical and organisational security measures in line with industry standards, including ISO 27001, 27017, 27018, 27701, PCI DSS. McAfee's Information Security & Privacy Management System (ISMS) ensures continued operation of sure measures, and supports the governance of information security & procession of personal data as a PII processor across all global locations and cloud services and is inclusive of the following sites with primary security operations:

- •McAfee, LLC. - 5000 Headquarters Drive, Plano, Texas 75024-5826 USA;
- •McAfee Ireland Limited - Building 2000, Citygate, Mahon, Cork City, Ireland, T12RRC9

In addition to any data security requirements set forth in the DPA, McAfee shall comply with the following, as derived from industry standards:

Standard	Control Ref/ Title		Control Description
ISO 27001 - Information Security Management System ***(incl. controls amendments for ISO 27017/27018/27701)***	***6.1.3 - A.5 Information Security Policy***		
	5.1.1	Policies for information security	A set of policies for information security is defined, approved by management, published and communicated to employees and relevant external parties.
	5.1.2	Review of the policies for information security	The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
	6.1.3 - A.6 Organization of Information Security		
	6.1.1	Information security roles and responsibilities	All information security responsibilities are defined and allocated.
	6.1.2	Segregation of duties	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
	6.1.3	Contact with authorities	Appropriate contacts with relevant authorities are maintained.
	6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.
	6.1.5	Information security in project management	Information security is addressed in project management, regardless of the type of the project.

	6.2.1	Mobile device policy	A policy and supporting security measures is adopted to manage the risks introduced by using mobile devices.
	6.2.3	Teleworking	A policy and supporting security measures is implemented to protect information accessed, processed or stored at teleworking sites.
	6.1.3 - A.7 Human Resource Security		
	7.1.1	Screening	Background verification checks on all candidates for employment is carried out in accordance with relevant laws, regulations and ethics and is proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
	7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors state their and the organization’s responsibilities for information security.
	7.2.1	Management responsibilities	Management requires all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
	7.2.2	Information security awareness, education, training	All employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
	7.2.3	Disciplinary process	There is a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
	7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated to the employee or contractor and enforced.
	6.1.3 - A.8 Asset Management		
	8.1.1	Inventory of assets	Assets associated with information and information processing facilities are identified and an inventory of these assets shall be drawn up and maintained.
	8.1.2	Ownership of assets	Assets maintained in the inventory are owned.

	8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.
	8.1.4	Return of assets	All employees and external party users return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
	8.2.1	Classification of information	Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
	8.2.2	Labelling of information	An appropriate set of procedures for information labelling is developed and implemented in accordance with the information classification scheme adopted by the organization.
	8.2.3	Handling of assets	Procedures for handling assets is developed and implemented in accordance with the information classification scheme adopted by the organization.
	8.3.1	Management of removal media	Procedures is implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
	8.3.2	Disposal of media	Media is disposed of securely when no longer required, using formal procedures.
	8.3.3	Physical media transfer	Media containing information is protected against unauthorized access, misuse or corruption during transportation.
	6.1.3 - A.9 Access Control		
	9.1.1	Access control policy	An access control policy is established, documented and reviewed based on business and information security requirements.
	9.1.2	Access to networks and network services	Users are only provided with access to the network and network services if they have been specifically authorized to use such services.
	9.2.1	User registration and de-registration	A formal user registration and de-registration process is implemented to enable assignment of access rights.

	9.2.2	User access provisioning	A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services.
	9.2.3	Management of privileged access rights	The allocation and use of privileged access rights is restricted and controlled.
	9.2.4	Management of secret authentication info of users	The allocation of secret authentication information is controlled through a formal management process.
	9.2.5	Review of user access rights	Asset owners review users' access rights at regular intervals.
	9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.
	9.3.1	Use of secret authentication information	Users are required to follow the organization's practices in the use of secret authentication information.
	9.4.1	Information access restriction	Access to information and application system functions is restricted in accordance with the access control policy.
	9.4.2	Secure log on procedures	Where required by the access control policy, access to systems and applications is controlled by a secure log-on procedure.
	9.4.3	Password management system	Password management systems is interactive and ensures quality passwords.
	9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.
	9.4.5	Access control to program source code	Access to program source code is restricted.
	6.1.3 - A.10 Cryptography		
	10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information is developed and implemented.
	10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys is developed and implemented through their whole lifecycle.

	6.1.3 - A.11 Physical and Environmental Security		
	11.1.1	Physical security perimeter	Security perimeters is defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
	11.1.2	Physical entry controls	Secure areas is protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
	11.1.3	Securing offices, rooms, facilities	Physical security for offices, rooms and facilities are designed and applied.
	11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents are designed and applied.
	11.1.5	Working in secure areas	Procedures for working in secure areas are designed and applied.
	11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
	11.2.1	Equipment siting and protection	Equipment are sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	11.2.2	Supporting utilities	Equipment are protected from power failures and other disruptions caused by failures in supporting utilities.
	11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage.
	11.2.4	Equipment maintenance	Equipment are correctly maintained to ensure its continued availability and integrity.
	11.2.5	Removal of assets	Equipment, information or software are not taken off-site without prior authorization.
	11.2.6	Security of equipment and assets off-premises	Security is applied to off-site assets taking into account the different risks of working outside the organization’s premises.
	11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media is verified to ensure that any sensitive data and licensed software has

			been removed or securely overwritten prior to disposal or re-use.
	11.2.8	Unattended user equipment	Users ensure that unattended equipment has appropriate protection.
	11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.
	6.1.3 - A.12 Operations Security		
	12.1.1	Documented operating procedures	Operating procedures are documented and made available to all users who need them.
	12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.
	12.1.3	Capacity management	The use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
	12.1.4	Separation of development, testing & operational environments	Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.
	12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware are implemented, combined with appropriate user awareness.
	12.3.1	Information backup	Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.
	12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed.
	12.4.2	Protection of log information	Logging facilities and log information are protected against tampering and unauthorized access
	12.4.3	Administrator and operator logs	System administrator and system operator activities are logged, and the logs are protected and regularly reviewed.
	12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain are synchronized to a single reference time source.

	12.5.1	Installation of software on operational systems	Procedures are implemented to control the installation of software on operational systems.
	12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used are obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
	12.6.2	Restrictions on software installation	Rules governing the installation of software by users are established and implemented.
	12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes.
	6.1.3 - A.13 Communications Security		
	13.1.1	Network controls	Networks are managed and controlled to protect information in systems and applications.
	13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.
	13.1.3	Segregation in networks	Groups of information services, users and information systems are segregated on networks.
	13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.
	13.2.2	Agreements on information transfer	Agreements address the secure transfer of business information between the organization and external parties.
	13.2.3	Electronic messaging	Information involved in electronic messaging is appropriately protected.
	13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information are identified, regularly reviewed and documented.
	6.1.3 - A.14 Systems Acquisition, Dev. & Maintenance		

	14.1.1	Information security requirements analysis & specification	The information security related requirements are included in the requirements for new information systems or enhancements to existing information systems.
	14.1.2	Securing application services on public networks	Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
	14.1.3	Protecting application services transactions	Information involved in application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
	14.2.1	Secure development policy	Rules for the development of software and systems are established and applied to developments within the organization.
	14.2.2	System change control procedures	Changes to systems within the development lifecycle are controlled by the use of formal change control procedures.
	14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.
	14.2.4	Restrictions on changes to software packages	Modifications to software packages are discouraged, limited to necessary changes and all changes are strictly controlled.
	14.2.5	Secure system engineering principles	Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.
	14.2.6	Secure development environment	secure development environments are established and are appropriately protected for system development and integration efforts to cover the entire system development lifecycle
	14.2.7	Outsourced development	The organization supervises and monitors the activity of outsourced system development.
	14.2.8	System security testing	Testing of security functionality is carried out during development.

	14.2.9	System acceptance testing	Acceptance testing programs and related criteria are established for new information systems, upgrades and new versions.
	14.3.1	Protection of test data	Test data is selected carefully, protected and controlled.
	6.1.3 - A.15 Supplier Relationship		
	15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed with the supplier and documented.
	15.1.2	Addressing security within supplier agreements	All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information
	15.1.3	Information communication technology supply chain	Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.
	15.2.1	Monitoring and review of supplier services	Supplier service delivery is regularly monitored, reviewed and audited.
	15.2.2.	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
	6.1.3 - A.16.1.3 Information Security Incident Management		
	16.1.1	Responsibilities and procedures	Management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents.
	16.1.2	Reporting information security events	Information security events are reported through appropriate management channels as quickly as possible.
	16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services are required to note and report any observed or suspected information

			security weaknesses in systems or services.
	16.1.4	Assessment of and decision on information security events	Information security events are assessed and are decided if they are to be classified as information security incidents.
	16.1.5	Response to information security incidents	Information security incidents are responded to in accordance with the documented procedures.
	16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents are used to reduce the likelihood or impact of future incidents.
	16.1.7	Collection of evidence	Procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence are defined and applicable.
	6.1.3 - A.17 Information Security Aspects of Business Continuity Management		
	17.1.1	Planning information security continuity	Requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster are determined.
	17.1.2	Implementing information security continuity	Processes and procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented and maintained.
	17.1.3	Verify, review and evaluate information security continuity	Established and implemented information security continuity controls are verified at regular intervals in order to ensure that they are valid and effective during adverse situations.
	17.2.1	Availability of information processing facilities	Information processing facilities are implemented with redundancy sufficient to meet availability requirements.
	6.1.3 - A.18 Compliance		
	18.1.1	Identification of applicable legislation & contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements are explicitly identified, documented and kept up to date for each information system and the organization.
	18.1.2	Intellectual property rights	Appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements

			related to intellectual property rights and use of proprietary software products.
	18.1.3	Protection of records	Records are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislation, regulatory, contractual and business requirements.
	18.1.4	Privacy and protection of Personal Data	Privacy and protection of personally identifiable information (Personal Data) are ensured as required in relevant legislation and regulation where applicable.
	18.1.5	Regulation of cryptographic controls	Cryptographic controls are used in compliance with all relevant agreements, legislation and regulations.
	18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.
	18.2.2	Compliance with security policies & standards	Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
	18.2.3	Technical compliance review	Information systems are regularly reviewed for compliance with the organization's information security policies and standards
ISO 27017 - Security Controls for Cloud Services	**CLD.6.3 - Relationship between cloud service customer & provider**		
	6.3.1	Shared roles & responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service are allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.
	8.1.5	Removal of cloud service customer assets	Removal of cloud service customer assets
	CLD.9.5 - Access control of CSP data in shared virtual environment		

	9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service is protected from other cloud service customers and unauthorized persons.
	9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment are hardened to meet business needs.
	12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment are defined, documented and monitored.
	12.4.5	Monitoring of cloud services	The cloud service customer has the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.
	13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks is verified based on the cloud service provider's network security policy.
ISO 27018 - Protection of Personal Data in Public Clouds, Acting as Personal Data Processors	**A.2 - Consent and choice**		
	A.2.1	Obligation to co-operate regarding Personal Data principals' rights	The public cloud Personal Data processor can provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of Personal Data principals’ rights to access, correct and/or erase Personal Data pertaining to them.
	A.3 - Purpose legitimacy and specification		
	A.3.1	Public cloud Personal Data processor's purpose	Personal Data to be processed under a contract is not processed for any purpose independent of the instructions of the cloud service customer.
	A.3.2	Public cloud Personal Data processor's commercial use	Personal Data processed under a contract is not used by the public cloud Personal Data processor for the purposes of marketing and advertising without express consent. Such consent is not a condition of receiving the service
	A.5 - Data minimization		
	A.5.1	Secure erasure of temporary files	Temporary files and documents are erased or destroyed within a specified, documented period
	A.6 - Use, retention, and disclosure limitation		
	A.6.1	Personal Data disclosure notification	The contract between the public cloud Personal Data processor and the cloud

			service customer requires the public cloud Personal Data processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of Personal Data by a law enforcement authority, unless such a disclosure is otherwise prohibited
	A.6.2	Recording of Personal Data disclosure	Disclosures of Personal Data to third parties is recorded, including what Personal Data has been disclosed, to whom and at what time.
	A.8 - Openness, transparency, and notice		
	A.8.1	Disclosure of sub-contracted Personal Data processing	The use of sub-contractors by the public cloud Personal Data processor to process Personal Data is disclosed to the relevant cloud service customers before their use.
	A.10 - Accountability		
	A.10.1	Notification of a data breach involving Personal Data	The public cloud Personal Data processor promptly notifies the relevant cloud service customer in the event of any unauthorized access to Personal Data or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of Personal Data.
	A.10.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures are retained for a specified, documented period upon replacement (including updating).
	A.10.3	Personal Data return, transfer and disposal	The public cloud Personal Data processor have a policy in respect of the return, transfer and/or disposal of Personal Data and make this policy available to the cloud service customer
	A.11 - Information security		
	A.11.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud Personal Data processor's control with access to Personal Data are subject to a confidentiality obligation.
	A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying Personal Data is restricted.
	A.11.3	Control and logging of data restoration	There is a procedure for, and a log of, data restoration efforts.

	A.11.4	Protecting data on storage media leaving the premises	Personal Data on media leaving the organization's premises is subject to an authorization procedure and is not accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).
	A.11.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption cannot be used except where it is unavoidable, and any use of such portable media and devices is documented.
	A.11.6	Encryption of Personal Data transmitted over public data-transmission networks	Personal Data that is transmitted over public data-transmission networks is encrypted prior to transmission
	A.11.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they are destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.
	A.11.8	Unique use of user IDs	If more than one individual has access to stored Personal Data, then they each have a distinct user ID for identification, authentication and authorization purposes
	A.11.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained.
	A.11.10	User ID management	De-activated or expired user IDs are not be granted to other individuals.
	A.11.11	Contract measures	Contracts between the cloud service customer and the public cloud Personal Data processor specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures are not subject to unilateral reduction by the public cloud Personal Data processor
	A.11.12	Sub-contracted Personal Data processing	Contracts between the public cloud Personal Data processor and any sub-contractors that process Personal Data specify minimum technical and

			organizational measures that meet the information security and Personal Data protection obligations of the public cloud Personal Data processor. Such measures are not subject to unilateral reduction by the sub-contractor.
	A.11.13	Access to data on pre-used data storage space	The public cloud Personal Data processor ensures that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.
	A.12 - Privacy compliance		
	A.12.1	Geographical location of Personal Data	The public cloud Personal Data processor specifies and document the countries in which Personal Data might possibly be stored.
	A.12.2	Intended destination of Personal Data	Personal Data transmitted using a data-transmission network is subject to appropriate controls designed to ensure that data reaches its intended destination.
ISO 27701 – Privacy Information Management System	**B.8.2 – Conditions for collection and processing**		
	B.8.2.1	Customer agreement	The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).
	B.8.2.2	Organization's purposes	The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
	B.8.2.3	Marketing and advertising use	The organization should not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization should not make providing such consent a condition for receiving the service.
	B.8.2.4	Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation

	B.8.2.5	Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.
	B.8.2.6	Records related to processing PII	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.
	B.8.3 – Obligations to PII principals		
	B.8.3.1	Obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations relating to PII principals
	B.8.4 – Privacy by design and privacy by default		
	B.8.4.1	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
	B.8.4.2	Return, transfer or disposal of PII	The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.
	B.8.4.3	PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
	B.8.5 PII sharing, transfer and disclosure		
	B.8.5.1	Basis for PII transfer between jurisdictions	The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.
	B.8.5.2	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.

	B.8.5.3	Records of PII disclosure to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.
	B.8.5.4	Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.
	B.8.5.5	Legally binding PII disclosures	The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.
	B.8.5.6	Disclosure of sub-contractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.
	B.8.5.7	Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.
	B.8.5.8	Change of subcontractor to process PII	The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.
Payment Card Industry Data Security Standard (PCI-DSS)	1	Firewall configuration to protect cardholder data	The installation contains a formal process for approving and testing all network connections and changes to the firewall and router configurations and complies with PCI-DSS standards. The firewall and router configurations restrict connections between untrusted networks and any system components in the cardholder data environment and prohibit direct public access between the Internet and any system component in the cardholder data environment. Security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties and include a personal firewall software.
	2	Do not use vendor-supplied defaults for system passwords and	Vendor-supplied defaults are changed, and McAfee removes or disables unnecessary default accounts before

		other security parameters	installing a system on the network. The configuration complies with standards that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. All non-console administrative access is encrypted using strong cryptography. Security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties
	3	Protect stored cardholder data	Cardholder data storage is kept to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage. Sensitive authentication data after authorization (even if encrypted) is not stored.
	4	Encrypt transmission of cardholder data across open, public networks	Use of strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public network.
	5	Use and regularly update anti-virus software or programs.	All anti-virus mechanisms are maintained as follows: - Are kept current, - Perform periodic scans - Generate audit logs which are retained per PCI DSS Requirement 10.7.
	6	Develop and maintain secure systems and applications	security vulnerabilities are identified, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.
	7	Restrict access to cardholder data by business need to know	Access to system components and cardholder data is limited to only those individuals whose job requires such access.
	8	Assign a unique ID to each person with computer access	User Management procedures are defined and implemented to ensure proper user identification management for non-consumer users and administrators on all system components as follows:

	9	Restrict physical access to cardholder data	Facility entry controls are used to limit and monitor physical access to systems in the cardholder data environment.
	10	Track and monitor all access to network resources and cardholder data	Audit trails are implemented to link all access to system components to each individual user.
	11	Regularly test security systems and processes	Processes are implemented to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
	12	Maintain a policy that addresses information security for all personnel	A security policy is established, published, maintained, and disseminated.

Annex 4 of SCHEDULE 1 - Authorized Third-Party Sub-processors

The current list of McAfee's Sub-processors is provided under https://www.mcafee.com/enterprise/en-us/assets/legal/enterprise-sub-processor-list.pdf.