Data Processing and Security Agreement for Suppliers

McAfee Supplier/Partner:

I would like to take this opportunity to express our appreciation to you and your employees for your outstanding services as part of our supply base. Your support and service are critical to our continued success in meeting our corporate objectives. Thank you!

It is an expectation that McAfee's suppliers and partners comply with all applicable data protection and data privacy laws. McAfee is committed to protecting the personal data of its employees, contractors, suppliers, customers and other third parties with whom it deals.

As you are certainly aware, international transfers of personal data have been through important changes throughout the last months – thus requiring amending our current data processing agreement and requesting you to complete the attached questionnaire.

Please note that – as of 27 September 2021, any transfer of McAfee Personal Data will be subject to the Module 2 of Standard Contractual Clauses available under https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en ("New SCCs"), which are deemed incorporated into our contractual relationship.

Also, the European Data Protection Board updated on 18 June 2021 its Recommendations 2020/1 and 2020/2 requesting additional measures to be taken on top of the set of Standard Contractual Clauses executed between our companies.

Henceforth, as a mandatory requirement, on top of completing the Annexes to the New SCCs, please review the attached questionnaire and provide us with the answers allowing us to assess if you transfer data to a country which does not provide the EU standard of essential equivalence, and if not the list of supplementary measures you use to bring the level of protection of the data transferred up to the EU standard of essential equivalence should you believe that the third country legislation to which you transfer McAfee Personal Data may impinge on the effectiveness of the transfer tool.

In addition, we would appreciate your confirmation of approval of these requirements, as well as a copy of your data transfer impact assessment, the availability of reports on any access requests received from public authorities and your commitment to assist data subjects in exercising their rights in the non-EEA jurisdiction through ad hoc redress mechanisms and legal counselling by countersigning this letter.

Please feel free to reach out to McAfee Privacy Office at protectprivacy@mcafee.com should you have any questions.

Sincerely,

Patrick Ryan
McAfee, LLC

McAfee Privacy Review Audit

Name of supplier/partner:
Address of supplier/partner:
Person completing this Audit/Exhibit DocuSign Form (your name, title, email address and phone number):
Name of McAfee Procurement/Sourcing/Chanel Manager:
Name and email address of Supplier/Partner Data Protection Officer:
Name of goods or service purchased:
Identify goods or services provided:
What personal data is collected from McAfee (including McAfee's customers and/ or personnel)?
What personal data is processed on behalf of McAfee?
Does the data include European Union (EU) or Argentinian personal data (yes or no)? Yes No
Does the data include personal data related to California Residents? Yes No
Is the personal data encrypted at rest? In transit? (If unknown, ask your InfoSec Dept.) Yes No
Purpose of processing personal data:
Where is the personal data stored?
What security is applied to protect the personal data (refer to article 32 of GDPR, Articles 33, 36 to 38 Regulation (EU) 2018/1725 or applicable privacy laws)?
From which countries is the personal data accessed?
What is the transfer mechanism used (i.e. – Standard Contractual Clauses, Argentine Model Clause, Binding Corporate Rules, ASEAN Model Contractual Clauses)?
Do you use any sub-processors / sub-contractors (refer to Article 28 of GDPR or to applicable privacy laws)? Yes No
If yes, please identify the sub-processors / sub-contractors used:
How long is the personal data retained for?
Is the solution/application you are providing McAfee, either on-premises at McAfee or a cloud-based offering?
General description of technical and organizational measures to protect personal data as provided in Article 32 in GDPR or under applicable privacy laws:
List of countries where the personal data is transferred
If the personal data concerns EU residents:

- On which transfer tool do you rely?
- Is anything in the law or practice of the third country to which you transfer McAfee Personal Data that could impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfers?
- Which supplementary measures necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence have you adopted?
- In particular, which specific measures do you take with respect to Law Enforcement Requests?
- Can you ensure that the countries to which you transfer McAfee EU Personal Data abide by laws and regulations on access to data by public authorities, including in the field of intelligence provided the legislation, that comply with the EDPB European Essential Guarantees, in the destination country?
- Do you include backdoors in your E2E products?
- Do you allow McAfee to conduct audits or inspections of the data processing facilities, on-site and/or remotely, to verify if data was disclosed to public authorities and under which conditions (access not beyond what is necessary and proportionate in a democratic society), for instance by providing for a short notice and mechanisms?
- Do you publish regular publication of transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law?

I confirm that the information I have provided is true and accurate. In addition, my company – and where provided for under local Data Protection Laws, my sub-processors - commit to assist data subjects in exercising their rights in the non-EEA jurisdiction through ad hoc redress mechanisms and legal counselling by signing below, in accordance with the requirements of applicable laws.

Supplier
Signature:
Printed Name:
Title:
Date:

McAfee

Supplier Data Processing and Security Exhibit (DPSE)

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

Unless you (hereinafter the "**Supplier**" or "**Data Importer**").) have entered into a valid agreement with McAfee, this Data Processing and Security Exhibit ("**DPSE**") is governed by and subject to the terms and conditions available at https://www.mcafee.com/content/dam/consumer/en-us/docs/legal/supplier-security-requirements.pdf (the "**Agreement**"), and is entered between Supplier and all its Affiliates and McAfee Ireland Limited on behalf of McAfee LLC and all of its Affiliates. McAfee and Supplier are collectively referred to as the "**Parties**".

In consideration of the mutual promises and covenants contained herein and of other good and valuable consideration, the receipt of which is hereby acknowledged, the Parties agree as follows:

Scope. This DPSE consists of this front page and the following terms:

Definitions

General Terms

Exhibit A: Technical and Organizational Measures

Exhibit B: Data Transfer Impact Assessment Questionnaire

Exhibit C: Supplemental Measures

Exhibit D: European Economic Area and Switzerland Standard Contractual Clauses

Exhibit E: Argentine Model Clauses

AS AGREED UPON BY each Party, through its authorized representative:

McAfee Ireland Limited on behalf of McAfee LLC and all its Affiliates	**Supplier on behalf of all its Affiliates**
Business Address:	Business Address:
Signature:	Signature:
Print Name:	Print Name
Title:	Title:
Date:	Date:

DEFINITIONS

All capitalized term shall have the meaning ascribed to them as set forth below.

"**Personal Data**", "**special categories of data**", "**process/processing**", "**Controller**", "**Processor**", "**Data Subject**" and "**supervisory authority**" shall have the same meaning as in the Applicable Law.

"**Adequacy Decision**" means a decision issued under Article 45 of the GDPR.

"**Affiliate**" means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity.

"Application Security" Refers to protecting data processed by an application, as well as the integrity and availability of services provided by the application.

"**APEC**" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information. "**APEC Member Economy**" means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

"**Argentine Model Clauses**" means the Model Agreement of International Transfer of Personal Data for the case of Provision of Services (*Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios*) (reference: EX-2016-00311578- -APN-DNPDP#MJ- Anexo II) approved by the *Dirección Nacional de Protección de Datos Personales* on 2 November 2016.

"**BCRs**" means the **Binding Corporate Rules** approved in accordance with Article 47 and 63 of the GDPR, which McAfee reserves the right to set in place and which, once approved, would be maintained throughout the term of the Agreement, or to the extent made available by the Supplier, which Supplier represents, warrants, and covenants maintaining during the full term of the Agreement.

"Business Critical" means loss that indirectly impacts a Mission Critical function, or directly impacts a business unit's primary function.

"**California Consumer Privacy Act of 2018**" or "**CCPA**" means Cal. Civ. Code § 1798.100, *et seq.*, as amended.

"**Data Protection Laws**" means EU Data Protection Laws, US Federal and State laws, including but not limited to the CCPA, the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018, the Asia-Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules ("CBPR") system and the Privacy Recognition for Processors ("PRP"), and, to the extent applicable, the data protection or privacy laws of any other country.

"**Data Subject**" means (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by the GDPR; or (ii) a "Consumer" as the term is defined in the CCPA.

"EEA" means the European Economic Area and Switzerland.

"**End-User Customers**" means McAfee's customers using McAfee products and services and McAfee's partners designated for the reselling and distribution of McAfee products and services.

"EU Data Protection Laws" means the GDPR and any local data protection laws applicable in the EEA.

"External Facing (Public)" means information available without approval or authentication.

"**GDPR**" means the European Union (EU) General Data Protection Regulation 2016/679.

"Information Security Incident" means any actual or reasonably suspected occurrence involving the compromise of the security, confidentiality, and/or integrity of McAfee Confidential Information through the accidental or unlawful destruction or loss of McAfee Confidential Information or the unauthorized collection, misappropriation, use, copying, modification, disposal, disclosure, or access of McAfee Confidential Information including Personal Data.

"MCCs" means the ASEAN Model Contractual Clauses approved on 22 January 2021 by the Digital Ministers of the Association of Southeast Asians Nations (ASEAN).

"Mission Critical" means a loss that directly impacts McAfee's ability to book, build, ship, order, pay, close or communicate with its End-User Customers.

"McAfee Confidential Information" means information with restricted access limited to those individuals with a need to know.

"Physical Security" means measures taken to protect systems, buildings and related support infrastructure against threats from the physical environment.

Personal Data shall have the same meaning as in the Data Protection Laws.

"**Regulator**" means either (as applicable): (i) an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR; or (ii) the California Attorney General.

"**SCCs**" means the EU Standard Contractual Clauses pursuant to European Commission Decision of 4 June 2021, and its Module 2 "Controller to Processor" incorporated herein by reference together with its Appendices attached hereto as Exhibit D.

"**Subprocessor**" means any processor engaged by the Supplier or by any other Subprocessor of the Supplier, which agrees to receive from the Supplier, or from any other Subprocessor of the Supplier, McAfee or End-User Customers' Personal Data exclusively with the intention for processing activities to be carried out on behalf of McAfee and in accordance with its instructions, the terms of the Agreement, this DPSE and the terms of the written subcontract.

"**Transfer**" means the transfer or disclosure or any other type of access to Personal Data to a person, organisation or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

"**Transfer Mechanism(s)**" means the BCRs, the SCCs, the MCCs, the Argentine Model Clauses and any other transfer mechanism required to undertake a Transfer under Data Protection Laws.

"Unsecured Area" means areas that are not controlled by physical access security measures. Some examples are the lobby of an access-controlled building or a warehouse delivery dock with PC access to corporate systems.

"Virtualized System" means any of the following: A virtual machine (VM) is a software implementation of a computer that executes programs like a real machine. The virtual machine monitor (VMM) or hypervisor is the software layer providing the virtualization. Platform virtualization and /or hardware virtual machines that allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system.

-General Terms follow this page-

GENERAL TERMS

1. DETAILS OF THE PROCESSING ACTIVITIES

McAfee shall be the Controller or the Processor for its own End-User Customers under the GDPR and a "business" under the CCPA (or similar concept under other Applicable Laws), and Supplier and supplier's sub-processors under the GDPR shall be the Processor regarding the Personal Data processed by Supplier on McAfee's behalf or sub-processed on behalf of End-User Customers ("**McAfee Personal Data**") and "service provider" as defined in CCPA section 1798.140 (v) (or similar concept under other Applicable Laws).

The details of the processing activities to be carried out by the Supplier under the Agreement and, the special categories of Personal Data where applicable, are specified in Exhibit B of this DPSE.

2. OBLIGATIONS OF THE SUPPLIER

The Supplier agrees and warrants:

(a) to process Personal Data only:

- on behalf of McAfee and in accordance with its documented instructions unless otherwise required by Data Protection Laws;
- for the sole purpose of executing the Agreement or as otherwise instructed by McAfee, and not for the Supplier's own purposes or other commercially exploitation. For clarity, Supplier will not collect, retain, use, or disclose McAfee Personal Data for any purpose other than as necessary for the specific purpose of processing McAfee Personal Data, including collecting, retaining, using, or disclosing McAfee Personal Data for a commercial purpose other than providing and enhancing McAfee Products and Services. This provision shall not apply to anonymized DDoS and traffic statistics that may be collected as long as such data is not reasonably related to, directly or in combination with other data, McAfee Personal Data, and Supplier shall not itself or allow others to make any attempt to derive Personal Data from such anonymized DDoS and traffic statistics. Supplier will not use McAfee Personal Data for the purpose of providing services to another person or entity except for the sole purposes of detecting data security incidents and protecting against fraudulent or illegal activity. Without limiting the foregoing, Supplier will not sell McAfee Personal Data; and
- in compliance with this DPSE; and
- in an encrypted (and where applicable, anonymized or pseudonymized) manner while in transit and storage and in accordance with the current state of the art encryption technology and industry best practice as available in the commercial marketplace;

(b) if it is legally required to process McAfee Personal Data otherwise than as instructed by McAfee, to notify McAfee and the Data subject before such processing occurs, unless the Data Protection Law requiring such processing prohibits the Supplier from notifying McAfee on an important ground of public interest, in which case it shall notify McAfee as soon as that Data Protection Law permits it to do so; and to take legal action against any disclosure of Personal Data and to refrain from disclosing the Personal Data to authorities or other third parties until a competent court of last instance has ordered the personal data to be disclosed.

(c) that it has implemented and will maintain appropriate technical and organisational measures to protect McAfee Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access and, in particular, where the processing involves the transmission of data over a network, against all other unlawful forms of processing.

Having regard to the state of the art and cost of their implementation, the Supplier agrees that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of McAfee Personal Data to be protected and will at a minimum include those measures described McAfee's

Standards "Supplier Security Requirements available under https://www.mcafee.com/enterprise/en-us/assets/legal/supplier-security-requirements.pdf, and as further detailed under **Exhibit A**;

(d) that protective devices are set up for ensuring the integrity and the authenticity of McAfee Personal Data, especially the state-of-the-art protective devices against malware and similar security attacks;

(e) that it has implemented measures to prevent McAfee Personal Data from undergoing any unwanted degradation or deletion without having a copy immediately usable;

(f) that it has a business continuity plan which includes measures to reduce unavailability of the services in the event of a lasting incident or security breach, and which includes service levels and maximum recovery response and resolution time charter to face any crisis scenario;

(g) that it will treat all McAfee Personal Data as confidential information and not disclose such confidential information without McAfee's prior written consent except:

- to those of its personnel who need to know the confidential information in order to carry out the Services; and
- where it is required by a court to disclose McAfee Personal Data, or where there is a statutory obligation to do so, but only to the minimum extent necessary to comply with such court order or statutory obligation;

(h) to take reasonable steps to ensure that its personnel who have access to the Personal Data:

- are subject to a code of conduct and an ethic guide substantially compliant with McAfee's code of conduct available at https://www.mcafee.com/content/dam/consumer/en-us/docs/legal/code-of-conduct.pdf?culture=EN-PH;
- are informed of the confidential nature of McAfee Personal Data and obliged to keep such McAfee Personal Data confidential; and
- are aware of and comply with the Supplier's duties and their personal duties and obligations under this DPSE;

(i) that it will promptly, and at least within **24 hours**, notify McAfee about:

- any instruction which, in its opinion, infringes applicable law;
- any Information Security Incident involving Supplier or its Subprocessors;
- any complaint, communication or request received directly by the Supplier or a Subprocessor from a data subject and pertaining to their Personal Data, without responding to that request unless it has been otherwise authorised to do so by McAfee; and
- any change in legislation applicable to the Supplier or a Subprocessor which is likely to have a substantial adverse effect on the warranties and obligations set out in this DPSE;

(j) that upon discovery of any Information Security Incident affecting McAfee Personal Data, it shall:

- immediately take action to prevent any further Information Security Incident; and
- provide McAfee with full and prompt cooperation and assistance in relation to any notifications that McAfee is required to make as a result of the Information Security Incident;

(k) to provide McAfee with full and prompt cooperation, at least **within 48 hours**, and assistance in relation to any complaint, communication or request received from a Data Subject, including by:

- providing McAfee with full details of the complaint, communication or request;

- where authorised by McAfee, complying with a request from a data subject in relation to their McAfee Personal Data within the relevant timescales set out by applicable law and in accordance with McAfee's instructions;
- providing McAfee with any McAfee Personal Data it holds in relation to a Data Subject, if required in a commonly-used, structured, electronic and machine-readable format;
- providing McAfee with any information requested by McAfee relating to the processing of McAfee Personal Data under this DPSE;
- correcting, deleting or blocking any McAfee Personal Data; and
- implementing appropriate technical and organisational measures that enable it to comply with this subsection (k);
- ensuring that the data subject has been informed or will be informed before, or as soon as possible after, their Personal Data is transmitted to a third country not providing adequate protection within the meaning of Applicable Laws;

(l) to provide McAfee with full and prompt cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that McAfee is legally required to make in respect of McAfee Personal Data;

(m) to appoint, and identify to McAfee, an individual to support McAfee in monitoring compliance with this DPSE and to make available to McAfee upon request all information and evidence necessary to demonstrate that the Supplier is complying with its obligations under this DPSE;

(n) at the request of McAfee, to submit its data processing facilities for audits and inspections of the processing activities covered by this DPSE, which shall be carried out by McAfee or a regulated End-User Customer, for example when a government or regulatory body with binding authority regulates such entity's regulated services such as banking for instance) or any independent or impartial inspection agents or auditors selected by McAfee or a regulated End-User Customer and not reasonably objected to by the Supplier, and to allow McAfee to provide any such reports to its End-User Customers where required.

(o) that it shall maintain the list attached hereto in Exhibit B of Subprocessors that may Process the Personal Data of Supplier's customers. Supplier shall require all Subprocessors to abide by the same obligations as Supplier under this Agreement. Supplier remains responsible at all times for compliance with the terms of this Agreement by Supplier Affiliates and Subprocessors. McAfee consents to Supplier's use of Supplier's Affiliates and Subprocessors in the performance of the Services. Supplier shall inform McAfee of any new Subprocessors Supplier intends to engage and will obtain prior written consent from McAfee. McAfee may object to the engagement of any new Subprocessor but shall not unreasonably withheld its consent to such appointment; Supplier shall specifically inform in writing McAfee of any intended changes of that list through the addition or replacement of subprocessors at least 30 days in advance, thereby giving McAfee sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). If McAfee has objections to the appointment of any new Subprocessor, the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, McAfee may terminate the part of the Service performed under this DPSE that cannot be performed by Supplier without use of the objectionable Subprocessor. Supplier shall refund any pre-paid, unused fees to McAfee with respect to the terminated part of the Services.

(p) upon request, to promptly send a copy of any data privacy, data protection (including, but not limited to, measures and certifications) and confidentiality portions of an agreement it concludes with a Subprocessor relating to McAfee Personal Data to McAfee;

(q) shall promptly notify McAfee should Supplier receive a request from a data subject to have access to Personal Data or any complaint or request relating to McAfee's obligations under applicable Data Protection Laws. McAfee is solely responsible for responding to such requests unless Supplier does not inform McAfee of the request, and Supplier will not respond to any such data subject unless required by applicable laws or unless instructed in writing by McAfee to do so;

(r) has no reason to believe that the laws and practices in the third country of destination applicable to the processing of the Personal Data, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under the SCCs. 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 SCCs;

(s) shall document the assessment under Clause 15 paragraph (b) of the SCCs and make it available to the competent supervisory authority on request of McAfee.

3. LIABILITY. Supplier shall remain fully liable to McAfee for any Subprocessors' processing of McAfee Personal Data under the Agreement. Notwithstanding anything contained in the Agreement to the contrary, nothing in the limitation of liability in the Agreement will be read or interpreted in any way to limit Supplier's liability for breach of this DPSE.

4. INTERNATIONAL DATA TRANSFER.

Without prejudice to any applicable Data Protection laws, no Transfer of Personal Data may take place to countries that have not received an Adequacy Decision or without having in place an adequate Transfer Mechanism.

Restricted transfers from the EEA. Where the Transfer to Supplier is covered by Supplier's BCR, Supplier warrants that it shall (i) promptly notify McAfee of any subsequent material changes in such authorization, and (ii) enter into an appropriate onward transfer agreement with any such Subprocessor, or by entering into SCCs, in each case providing the same or more protection than the terms in this DPSE. If Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is Transferred by McAfee to Supplier in a country that has not been found to provide an adequate level of protection under Applicable Laws, then to the extent the Transfer is not covered by BCRs, any Transfer will be governed by the SCCs incorporated herein by reference, and the Appendices attached hereto as **Exhibit D**.

Data Transfer Impact Assessment Questionnaire. Supplier agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire executed by Supplier during its on-boarding process, and acknowledges that this Questionnaire is deemed incorporated herein as **Exhibit B**.

Data Transfer Impact Assessment Outcome. Taking into account the information and obligations set forth in the DPSE, its Exhibits (including the Supplemental Measures completed by Supplier during its on-boarding process, and deemed incorporated as **Exhibit C**, and, as may be the case for a party, McAfee's independent research, to the parties' knowledge, the Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the SCCs attached hereto to a country that has not been found to provide an adequate level of protection under Applicable Laws is afforded a level of protection that is essentially equivalent to that guaranteed by Applicable Laws.

Restricted Transfers from Argentina. To the extent a Transfer involves Argentinian Personal Data to Supplier or its Sub-processors located outside Argentina, such Transfer will be governed by the Argentine Model Clauses incorporated herein by reference and its Appendix attached hereto as **Exhibit E**.

Restricted transfers from other jurisdictions. Transfers from other jurisdictions globally that have Transfer restrictions are subject to the terms of this DPSE or to the mandatory terms required under local Applicable Laws of such Transfer restrictions documentation (such as, but not limited to the MCCs), including any data protection and security policies referenced herein.

Subprocessors. Supplier will provide without undue delay McAfee with a copy of the relevant Transfer Mechanism and/or related Data Processor provisions with its Subprocessors upon request. McAfee shall be entitled to terminate the Agreement if the approved Transfer Mechanism is invalidated and no alternative approved Transfer Mechanism is put in place, or if the related Data Processing provisions with its Subprocessors do not comply with this DPSE.

In the event of inconsistencies between the provisions of the Transfer Mechanisms and this DPSE or the Agreement, said Transfer Mechanisms shall take precedence to the extent required by Data Protection Laws. In the event that such Transfer Mechanisms are amended, replaced or repealed under Data Protection Laws, or in the event new Transfer Mechanisms terms are adopted under Data Protection Laws, the parties shall deem such Transfer Mechanisms deemed as incorporated herein by reference, and shall work together in good faith to enter into any required updated version or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws. This DPSE supersedes any and all prior understandings and agreements relating to the protection of data and compliance with Data Protection Laws and the express provisions of this DPSE control over any other agreement or amendment.

Supplier's privacy practices comply with the Asia-Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules ("CBPR") system and the Privacy Recognition for Processors ("PRP"). The APEC CBPR system provides a framework to ensure protection of personal data transferred among participating APEC economies and the PRP demonstrates an organization's ability to provide effective implementation of a personal data controller's privacy obligations related to the processing of personal information.

5. INDEMNITY. The Supplier shall indemnify and keep indemnified and defend at its own expense McAfee against all costs, claims, damages or expenses incurred by McAfee or for which McAfee may become liable due to any failure by the Supplier or its employees or agents to comply with any of its obligations under this DPSE.

Additional Terms for Individual Remedies. To the extent required under local applicable Data Protection Laws, Supplier and its subprocessors will provide data subjects with direct rights of enforcement of the Transfer Mechanisms.

6. ALLOCATION OF COSTS. Other than with respect to the Indemnity provisions in section 5 above, each party shall perform its obligations under this DPSE at its own cost.

7. TERM AND TERMINATION OF THE SERVICES.

The parties agree that McAfee Personal Data will be processed by the Supplier for the duration of the Services under the Agreement.

The parties agree that upon termination of the Services in so far as they relate to McAfee Personal Data, the Supplier and all Subprocessors shall, at the choice of McAfee , return all McAfee Personal Data and the copies thereof to McAfee , or securely destroy all McAfee Personal Data and certify to McAfee that it or they have done so, unless Data Protection Laws to which the Supplier or a Subprocessor are subject prevent the Supplier or Subprocessor from returning or destroying all or part of McAfee Personal Data. Where Data Protection Laws prevent the Supplier or Subprocessor from returning or destroying McAfee Personal Data, the Supplier warrants that it will guarantee the confidentiality of McAfee Personal Data and will not actively process McAfee Personal Data for any purpose not required under Data Protection Law, and will guarantee the return and/or destruction of McAfee Personal Data as requested by McAfee when the legal obligation to not return or destroy the information is no longer in effect.

8. RECORDS AND PROOFS.

Supplier warrants it keeps records concerning its security, and organizational technical measures as well as records on any security incident affecting McAfee Personal Data. Such records shall be made available in a standard format immediately exploitable and available for inspection, upon McAfee's request in the course of a security check or in the framework of an audit.

9. TERM, PORTABILITY AND REVERSIBILITY AND SURVIVAL

This DPSE shall remain in full force as long as the Services Agreement remains in full force. In order to ensure portability of the McAfee Personal Data, and should the Services Agreement be terminated for any reason, Supplier shall, within five (5) days of McAfee's request, make available McAfee Personal Data in a standard format. Such Information shall include account level information including IP addresses, hostnames, infrastructure information and McAfee contact information.

Survival. Any terms of this DPSE which by their nature should survive the termination of this DPSE shall survive such termination, including, without limitation, the indemnity and liability terms herein in section 5 and 6.

10. STANDARD CONTRACTUAL CLAUSES.

By executing this DPSE, Supplier is deemed to execute the Standard Contractual Clauses as set out in the Exhibits below.

11. MISCELLANEOUS.

In the event of inconsistencies between the provisions of this DPSE and the Services Agreement, the provisions of this DPSE shall prevail with regard to the parties' data protection obligations relating to McAfee Personal Data. In cases of doubt, this DPSE shall prevail, in particular, where it cannot be clearly established whether a clause relates to a party's data protection obligations.

Should any provision or condition of this DPSE be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this DPSE shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this DPSE to the maximum extent permitted by law. The provision or condition affected shall be construed either: (i) to be amended in such a way that ensures its validity, lawfulness and enforceability while preserving the parties' intentions, or if that is not possible, (ii) as if the invalid, unlawful or unenforceable part had never been contained in this DPSE.

Any amendments to this DPSE shall be in writing duly signed by authorised representatives of the parties hereto.

12. BCRS.

If at any time after the Effective Date, McAfee elects to use BCRs, McAfee shall transfer Personal Data in accordance with its BCR, and McAfee will be regarded as the Data Exporter and the Supplier will be regarded as the Data Importer. Once approved, McAfee shall maintain such BCR's throughout the term of the Agreement. Should McAfee cease to abide by such BCR's, the Parties will agree not to transfer any Personal Data outside the appropriate mechanisms provided under Sections 44 through 50 of the GDPR.

EXHIBIT A – Technical and Organizational Measures

The technical and organisational measures detailed under https://www.mcafee.com/content/dam/consumer/en-us/docs/legal/supplier-security-requirements.pdf are deemed incorporated herein, and summarizes the technical, organisational and physical security measures implemented by the Supplier.

EXHIBIT B – Data Transfer Impact Assessment Questionnaire

The Data Transfer Impact Assessment Questionnaire completed during Supplier's on-boarding process is deemed incorporated herein.

This Exhibit B forms part of the DPSA. Capitalized terms not defined in this Exhibit B have the meaning set forth in the DPSA.

1. What countries will McAfee Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.
    a. **Answer:** [Partner to insert response].
2. What are the categories of data subjects whose McAfee Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
    a. **Answer:**
        1. Current, former, prospective employees.
        2. Current, former, prospective employees and their dependents.
        3. where applicable Employees of Corporate customers
        4. where applicable McAfee consumer customers and former consumer customers
        5. Customer contacts
3. What are the categories of McAfee Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
    a. **Answer:**

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

        1. Employees' names and contact information, including addresses, emails, phone numbers, IP addresses, employment history, education/qualifications, transaction history.
        2. Employees' names and contact information, including addresses, emails, phone numbers, IP addresses; employees' dependents' names and contact information, including addresses, emails, phone numbers, transaction history.
        3. McAfee Corporate customers' employees' names and business contact information, including addresses, emails, phone numbers, IP addresses, transaction history, payment information.
        4. Customer contacts, including employees' names and business contact information, including addresses, emails, phone numbers, IP addresses, transaction history, payment information.
4. Will any McAfee 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 be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures?
    a. **Answer:**

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

1. None.
2. 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:

5. What business sector is Partner involved in?
    a. **Answer:** [Partner to insert response].
6. Broadly speaking, what are the services to be provided and the corresponding purposes for which McAfee Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
    a. **Answer:** The Data Importer is the Partner on behalf of itself and its Affiliates worldwide ("Data Importer"). The Data Importer provides products and/or services to the Data Exporter in relation to the Agreement, in the course of which it processes certain personal data as a processor.
7. What is the frequency of the transfer of McAfee Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is McAfee Personal Data transferred on a one-off or continuous basis?
    a. **Answer:** [Partner to tick as applicable:]

    ☐ None.

    ☐ One-off.

    ☐ On-going.

    ☐ In accordance with the specifications described under the Agreement.
8. When McAfee Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Partner, how is it transmitted to Partner? Is McAfee Personal Data in plain text, pseudonymized, and/or encrypted?
    a. **Answer:** Partner will adhere to the security requirements listed in Exhibit A with respect to any transfer of McAfee Personal Data
9. What is the period for which the McAfee Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?
    a. **Answer:** [Partner to insert response:]

    ☐ Limited to the term of the Agreement.

    ☐ Other. Please specify _____

    ☐ criteria used to determine that period. Please specify: _____

10. Please list the Subprocessors that will have access to McAfee Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

    [To Partner: Please complete the below by inserting name, address and services provided by 3rd party Sub-processors and Affiliates. If this Appendix remains unfilled, Partner is deemed not to be using any Subprocessor.]

Name of Subprocessor	Subject matter, nature, and duration of processing	Location (Country)	Adequacy Mechanism Supporting Transfer
[Partner to complete].			

11. Is Partner subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where McAfee Personal Data is stored or accessed from that would interfere with Partner fulfilling its obligations under either of the attached set(s) of Standard Contractual Clauses? For example, FISA 702 or U.S. Executive Order 12333. If yes, please list these laws.

    a. **Answer:** [Partner to insert response].

12. Has Partner ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.

    a. **Answer:** [Partner to insert response].

13. Has Partner ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

    a. **Answer:** [Partner to insert response].

14. What safeguards will Partner apply during transmission and to the processing of McAfee Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?

    a. **Answer:**

EXHIBIT C – Supplemental Measures

This Exhibit C forms part of the DPSE. Capitalized terms not defined in this Exhibit C have the meaning set forth in the DPSE.

Supplier has a duty to not comply with (more than just challenge) FISA requests or another order that would violate EU law, or alternatively, and further agrees not to use a specific subprocessor and/or send data to one of the countries outlined in Exhibit B.

[Please insert any other supplemental measure, as appropriate.]

EXHIBIT D – European Economic Area And Switzerland Standard Contractual Clauses

This Exhibit D forms part of the DPSE.

SECTION I

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) 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.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(f) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply *mutatis mutandis* to the Parties processing of personal data that is subject to the United Kingdom General Data Protection Regulation as supplemented by terms in the Data Protection Act 2018.

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.

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

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.

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.

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.

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

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.

MODULE TWO: Transfer controller to processor

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 (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.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(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 thirty (30) days 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. 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.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(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.

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.

MODULE TWO: Transfer controller to processor

(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.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(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.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State, the following section applies: 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(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.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

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.

SECTION IV – FINAL PROVISIONS

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) 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.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

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.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(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.

APPENDIX

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: McAfee.

Address: As set forth in the front page of the DPSE.

Contact person's name, position and contact details: As set forth in the front page of the DPSE

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

Role (controller/processor): Controller.

Data importer(s):

2. Name: Supplier.

Address: As set forth in the front page of the DPSE.

Contact person's name, position and contact details: As set forth in the front page of the DPSE

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

As set forth in Exhibit B.

Categories of personal data transferred

As set forth in Exhibit B.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As set forth in Exhibit B.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As set forth in Exhibit B.

Nature of the processing

As set forth in Exhibit B.

Purpose(s) of the data transfer and further processing

As set forth in Exhibit B.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As set forth in Exhibit B.

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

As set forth in Exhibit B.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer shall implement and maintain appropriate technical and organisational measures that protect personal data in accordance with the DPSE.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPSE.

ANNEX III

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Clauses are dated as of the same date as the DPSE.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors. This Addendum forms part of and supplements **Exhibit D**. If Personal Data originating in the United Kingdom is transferred by Customer to McAfee in a country that has not been found to provide an adequate level of protection under UK Data Protection Laws, the Parties agree that said transfer shall be governed by the Clauses as supplemented by this Addendum.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses.
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland.

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 UK GDPR.
5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:
    a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and
    b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.
9. The amendments required by Section 8 above, include (without limitation):
    a. References to the "Clauses" means this Addendum as it incorporates the Clauses
    b. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

    c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
    d. References to Regulation (EU) 2018/1725 are removed.
    e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"
    f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
    g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
    h. Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

EXHIBIT E – ANNEX A TO ARGENTINE MODEL CLAUSES

Titulares de los datos	Data owners
Los datos personales transferidos se refieren a las siguientes categorías de titulares de los datos:	The personal data transferred concern the following categories of data owners:
	Refer to Exhibit B of this DPSE
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*
	Refer to *Exhibit B of this DPSE*
Características de los datos	Characteristics of the data
Los datos personales transferidos se refieren a las siguientes categorías de datos:	The personal data transferred concern the following categories of data:
	Refer to Exhibit B of this DPSE
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*
Tratamientos previstos y finalidad	*Refer to Exhibit B of this DPSE*
	Purpose of the data processing to be conducted:
Los datos personales transferidos serán sometidos a los siguientes tratamientos y finalidades:	The transferred personal data will be subject to the following processing and purposes:
	Please refer to the attached "Description of Transfer" document(s)
Consulte *La descripción de la transferencia* adjunta.	*Refer to Exhibit B of this DPSE*

Data Importer

By:

Name:

Name of the Supplier:

Title

Address and Country of Supplier: