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.

This Data Processing and Security Exhibit ("**DPSE**") is incorporated into and forms part of the Master Services Agreement (the "**Agreement**") between _____ ("**Supplier**") and McAfee, 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 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

Capitalized terms shall have the meaning ascribed to them as set forth below. Capitalized terms not defined below have the meaning ascribed to them in the Agreement.

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

"**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.

"**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 or other applicable U.S. Data Protection Laws.

"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.

"**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).

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

"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; (ii) the California Privacy Protection Agency; or (iii) the Attorney General of a U.S. state with authority to enforce applicable Data Protection Laws.

"**SCCs**" means "Module Two: Transfer controller to processor" of the Standard Contractual Clauses set forth in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, made avail-able at https://eur-lex.europa.eu/eli/dec_impl/2021/914/, as supplemented and/or amended by the selections and addendum set forth in Exhibit D below.

"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.

-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 the Services under the Agreement. 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) that 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/content/dam/consumer/en-us/docs/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 any independent or impartial inspection agents or auditors selected by McAfee and not reasonably objected to by the Supplier;

(o) that it shall maintain the list attached hereto in Exhibit B of Subprocessors that may Process McAfee Personal Data. 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) it 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 remains 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 or violation of applicable Data Protection Laws.

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 McAfee, without undue delay, 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 or applicable Data Protection Laws.

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

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.

10. 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.

11. STANDARD CONTRACTUAL CLAUSES.

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

12. 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 must be in writing and duly signed by authorised representatives of the parties hereto.

13. [INTENTIONALLY OMITTED]

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

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/Channel 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:

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 – EU STANDARD CONTRACTUAL CLAUSES SELECTIONS AND ADDENDUM

This Exhibit D forms part of the DPSE.

Section I, Clause 7 (Docking clause) - The docking clause is omitted by the Parties and shall not apply.

Section II, Clause 9(a) (Use of sub-processors) – Option 2 "General Written Authorization" shall apply, pursuant to the time period specified in Section 2(o) of the DPSE.

Section II, Clause 11 (Redress) – The optional wording in Clause 11(a) shall not apply.

Section IV, Clause 17 (Governing law) – The laws of the Republic of Ireland.

Section IV, Clause 18 (b) (Choice of forum and jurisdiction) – The courts of the Republic of Ireland.

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):

1. 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, as more fully described in Exhibit A to 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

Addendum To The Standard Contractual Clauses

A reference to a Clause in this *Annex III* shall be a reference to a Clause of the SCCs.

McAfee and Supplier agree that the SCCs shall be modified and/or supplemented as follows:

1. *Transfers from Switzerland.* If the SCCs apply to the Processing of Personal Data originating from Switzerland, the SCCs shall be modified as follows:

    a. the term "*member state*" shall not be interpreted in such a way as to exclude data subjects in Switzerland from suing for their rights in their place of habitual residence in accordance with Clause 18(c);

    b. the SCCs shall also protect the data of legal entities until the entry into force of the revised FDPA;

    c. references to the GDPR or other governing law contained in the SCCs shall also be interpreted to include the FDPA;

    d. the parties agree that the supervisory authority as indicated in Annex I.C shall be the Swiss Federal Data Protection and Information Commissioner;

    e. until the entry into force of the revised Swiss FDPA, the SCCs will also protect Personal Data of legal entities and legal entities will receive the same protection under the SCCs as natural persons.

2. *Transfers from the United Kingdom.* This Section shall apply to and modify the SCCs to the extent that UK Data Protection Laws apply to McAfee's Processing of Personal Data when it makes a Restricted Transfer of Personal Data to Supplier. As used in this Section, "Approved Addendum" means the template addendum issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 thereof. The Parties acknowledge and agree that:

        a. the information required to be set forth in "Part 1: Tables of the Approved Addendum" shall be completed in accordance with *Annex I* above; and

        b. "Part 2: Mandatory Clauses" of the Approved Addendum, as it is revised under Section 18 thereof, is incorporated herein by reference. For purposes of Section 19 of the Approved Addendum, McAfee may end the Approved Addendum in accordance with Section 19 thereof.

3. *Supplemental Business-Related Clauses.* In accordance with Clause 2, the Parties wish to supplement the SCCs with business-related clauses, which shall neither be interpreted nor applied in such a way as to contradict the SCCs (whether directly or indirectly) or to prejudice the fundamental rights and freedoms of Data Subjects. The Parties therefore agree that the applicable terms of the Agreement and this DPA shall apply if, and to the extent that, they are permitted under the SCCs, including without limitation the following:

a. In the event of a data subject request for a copy of the clauses in accordance with Clause 8.3, each Party agrees to make all redactions reasonably necessary to protect business or trade secrets or other confidential information of the other Party.

b. The termination provision(s) of the Agreement shall apply to a termination pursuant to Clause 14(f) or Clause 16.

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: