Trend Micro Ireland Limited

Transfer Impact Assessment – United States of America

Part 1: Know Your Transfers		
A. Assessment of the data importer		
1.	*Who is the exporter of the data (the "**data exporter**")?* *Please provide their name, contact details and any other information you consider relevant.*	Trend Micro Ireland Limited
2.	*Who is the importer of the data (the "**data importer**")?* *Please provide their name, contact details and any other information you consider relevant.*	Trend Micro Incorporated 225 East John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA
3.	*What does the data importer do?* *Provide details of the product or service they will provide.*	Hosting of the Smart Protection Network database with information about potentially malicious or harmful code or files and other associated information or data that may be related to unauthorized intrusions or attacks by malicious third parties including malicious IP addresses/domain names, some of which could contain very limited personal data.

		Provision of software support services to customers. Customers who install or use Trend Micro software may, if they choose to do so, configure the software to contribute to and consult this database. Customers who consult and contribute to this database will have their data sent to the US. Data contributed to this database will be encrypted.
4.	*Where (in what country or countries) will the data importer process the data?*	United States of America
5.	*Is the data importer a group company?*	☒ Yes ☐ No If no, is the data importer: ☐ A public authority ☐ A private enterprise (i.e. a company) ☐ A not-for-profit
6.	*Why will the data importer process the personal data? Please explain what processing activities the data importer will perform.*	To provide centralised hosting services for Trend Micro's database of malicious files/code etc. To provide software support services to Trend Micro's customers. Support personnel need to analyse product data logs and reports to assess and resolve support issues raised by its customers. .
7.	*Why are these transfers necessary? Could the instead processing be conducted in the European Economic Area ("**EEA**") (for EEA data) or the UK (for UK data)?*	Because this is a centralized database that was set up some years ago, in 2014, and the centralization is required to service global customers more efficiently. Trend Micro support cases are initially managed by local support personnel. Depending on the complexity of a case, it may be escalated to a product support engineer in the US.
8.	*Has a DPIA been conducted for the data importer's processing?* *If no, why not?*	☐ Yes, a DPIA has been conducted and is available at ☒ No, a DPIA has not been conducted because the processing is not "high risk" within the meaning of Art 35 GDPR)
9.	*Will the data importer onward transfer the personal data to other third parties?*	☒ Yes ☐ No

<table>
<tr><td></td><td>If so, please complete the table to (i) identify all such third parties and their location; identify why they will receive and/or process the personal data; and (iii) confirm whether Transfer Impact Assessments have been carried out in each case and where those Transfer Impact Assessments can be found (e.g. internal document management system number)?

(EDPB Recommendations: para.33)

Note: Both "transfer" and onward transfer" include remote access. Onward transfer can be to the same or another third country.</td><td>If yes, please provide details below:<table><tr><th>Third party recipient details (including name and location)</th><th>Why will it process the data?</th><th>Where will it process the data?</th></tr><tr><td>Amazon Web Services, Inc., USA

Amazon Web Service, Inc., Japan

Salesforce, USA

Microsoft Azure, Europe</td><td>Hosting for the SPN database

Hosting for the support logs

Hosting for the support database

Hosting for the support logs and remote access</td><td>US

Japan

US

Europe</td></tr></table></td></tr>
<tr><td>10.</td><td>If there are onward transfers to <u>other third parties</u>, please confirm whether Transfer Impact Assessments have been carried out in each case and where those Transfer Impact Assessments can be found (e.g. internal document management system number)?</td><td>☐ Yes, TIAs have been conducted and are available at

☒ No, TIAs have not been conducted because the recipients' security and supplementary measures have been reviewed, and each recipient has updated its data processing addendum incorporating processor to processor standard contractual clauses to enable onward transfers to it under Clause 18.6 of the 2021 EU standard contractual clauses.

See data processing addendum for: AWS, Salesforce and Microsoft Azure.</td></tr>
<tr><td colspan="3">B. Assessment of the data transferred</td></tr>
<tr><td>11.</td><td>What categories or types of data are being transferred?</td><td>Potentially malicious or harmful code or files and other associated information or data that may be related to unauthorized intrusions or attacks by malicious third parties, including malicious IP addresses/domain names, some of which could contain very limited personal data.

Personal data contained in support requests, which may include: name, email address, data logs, filename, filepath, URL, IP address.</td></tr>
</table>

11a.	*Can one or more of the following questions be answered with "Yes"?* • *The data does not include both name and address, and it does not include any ID numbers (passport, social security, etc); or* • *The data is fully anonymised by aggregation; or* • *The data is pseudonymised (including by encryption - EDPB Recommendations: para.33) and the key remains protected in the EEA/UK?*	☐ Yes ☒ No
11b.	*Is the data to be transferred of such a nature that it is unlikely to be of interest to third country government authorities? For example, ordinary commercial information like employee/HR, customer, or sales records.*	☒ Yes ☐ No
12.	*Does the data include communications contact information such as telephone numbers, email addresses or physical addresses?*	☒ Yes ☐ No If yes, which categories? ☐ Telephone numbers ☒ Email addresses ☐ Physical addresses
13.	*Does the data include telephone, email or other wire or electronic communications content or communications metadata?*	☒ Yes ☐ No If yes, which categories of communications content or metadata? ☐ Telephone content and/or metadata ☒ Email content and/or metadata ☒ Other wire or electronic communications and/or metadata
14.	*Does the data include special categories of data?*	☐ Yes ☒ No If yes, which categories of special category data: ☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs

		☐ Trade union membership ☐ Genetic data ☐ Biometric data used for unique identification ☐ Health data (including physical and mental health) ☐ Data about sex life or sexual orientation
14a.	*If the data includes special category data, can one or more of the following questions be answered with "Yes"?* • *The data does not provide any substantial insight into the individual's special category data or status, e.g. health data only about a minor cold.* • *The data can be collected easily through publicly available sources, e.g. public social media.* *The data can lead to no more than general assumptions about the individual, e.g. inferring possible ethnicity from names.*	N/A
15.	*Does the data include data about any individuals' criminal convictions and offences?*	☐ Yes ☒ No If yes, please explain why:
16.	*Is the data otherwise inherently sensitive data about individuals (e.g. their banking or other financial data) or likely to be of interest to government security or surveillance authorities?*	☒ Yes ☐ No If yes, please explain why: Data may be "of interest to government security or surveillance authorities": IP addresses and domain names of C&C servers may be shared with law enforcement authorities.
16a.	*In the case of financial data only, can it be said that the financial data does not provide any substantial insight to the individual's financial information or status (e.g. the fact that a person is the customer without further details, or bank account numbers only without balances)?*	N/A
17.	*Will this be a 'one-off' transfer or an ongoing series of transfers?*	☐ One-off or very few transfers ☒ Ongoing
17a.	*Will the importer have access to the transferred data only for a very short duration?*	☐ Yes ☒ No

18.	*Approximately how many data subjects' personal data will be transferred? If it is impossible to estimate numbers due to volume, please reply "Large scale transfer".*	Large scale transfer

Part 2: Identify the transfer tool relied upon		
19.	*Is the transfer being made to an importing territory or organisation that benefits from a European Commission adequacy decision (or, for UK data, adequacy regulations issued by the UK Secretary of State)?* *I.e. is it made to: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom or Uruguay?*	☐ Yes ☒ No If Yes, please note that it is <u>not</u> necessary to complete the rest of this form.
20.	*Is the transfer made on the basis of "appropriate safeguards" under Article 46 - i.e. reliance on EU Standard Contractual Clauses, Binding Corporate Rules, or similar? If so, please specify which safeguards will be relied upon.*	☒ SCCs ☐ BCR ☐ Approved code/ certification – please specify which: ☐ Other – please specify:
21.	*Is the transfer made in reliance upon a derogation under Art 49? If so, please specify which derogation is relied upon and why.*	☐ Explicit consent from data subjects ☐ Necessary for the performance of a contract with the data subject (or the implementation of pre-contractual measures taken at the data subject's request) ☐ Necessary for the conclusion or performance of a contract concluded in the interest of the data subject ☐ Necessary for important reasons of public interest ☐ Necessary for the establishment, exercise or defence of legal claims ☐ Necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent ☐ the transfer is made from a publicly-available register ☐ The transfer is not repetitive, concerns only a limited number of data subjects, and is necessary for the purposes of compelling legitimate

		interests provided the supervisory authority is informed of the transfer. Legal team must be consulted. Please indicate why you are relying on the above derogation:

Part 3: Is the transfer tool relied upon effective in light of the circumstances of the transfer?		
22.	*Has the importing territory implemented legislation or executive powers that enables government authorities access to data exporters' personal data e.g. for surveillance, intelligence, national security, criminal law enforcement and other regulatory purposes, whether through the data importer or telecommunication providers or communication channels?* *Please provide an overview of each of these applicable laws, regulations and practices as well as a description of how authorities in the importing territory can rely on them.*	☒ Yes ☐ No ☐ Somewhat Please provide details: • **Pursuant to s. 702 FISA**, the United States government ("**USG**") can compel "electronic communications service providers" to disclose information about non-US persons located outside the US for the purposes of foreign intelligence information gathering. This information gathering is jointly authorised by the US Attorney General and the Director of National Intelligence, and must be approved by the Foreign Intelligence Surveillance Court in Washington, DC. Once approved, USG sends relevant providers certain "selectors" (such as telephone numbers or email addresses) associated with specific "targets" (such as a non-US person or legal entity). In-scope providers must comply with these directives in secret and are not allowed to notify their users. In-scope providers are electronic communication service providers (**"ECSP"**) within 50 U.S.C § 1881(b)(4), namely: electronic communication service providers (**"ECS"**) and remote computing service providers (**"RCS"**), as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711; a telecommunications carrier, as defined in 47 U.S.C. §153 – i.e., a provider that has traffic flowing through its internet backbone and that carries traffic for third parties other than its own customers; any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; and any other relevant U.S. entity that is an officer, employee, or agent of one of the entities described above. • **Pursuant to Executive Order 12333 ("EO12333")**, USG authorises intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may include accessing underwater cables carrying Internet data in transit to the United States. EO12333 does not rely on the compelled assistance of service

		providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure. • **Pursuant to the Electronic Communications Privacy Act ("ECPA")**, all ECS and RCS may or must disclose user/subscriber records and communications, both to law enforcement and private parties. Generally, ECPA restricts when ECS and RCS can freely disclose information. Communications content (email, private messages, photographs, etc.) is generally subject to the strictest rules, and "basic" subscriber information (name of account holder, types of service they receive, etc.) are provided the least protection. An ECS/RCS can be subject to various types of legal process (subpoena, 2. 18 U.S.C. 2703(d) court order, court-issued ECPA warrant, pen register and trap and trace court order and court-issued Title III Wiretap), each of which is either issued by a court or otherwise subject to judicial oversight. An ECS or RCS may be compelled to produce data to U.S. law enforcement for criminal investigative purposes if such data is within its possession, custody, or control regardless of whether such data is stored within or outside of the United States and often regardless of whether the ECS or RCS itself is in physical possession of the data. • **National Security Letters ("NSLs")** can be issued without judicial oversight under ECPA, the Fair Credit Reporting Act, and the Right to Financial Privacy Act. The USG must certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.
23.	***European Essential Guarantees for Surveillance Measures - Guarantee 1:*** *Is any such government access defined by clear, precise and publicly-accessible rules and legislation?* *I.e. is access to the transferred personal data and further use of such data by public authorities in the importing territory based on clear, precise and accessible law as to its scope and application (as opposed to the discretionary powers that authorities may have)?*	☐ Yes ☒ No ☐ Somewhat Please provide details: • In relation to FISA and EO 12333. The CJEU held in the Schrems II judgement that FISA 702 and EO 12333 "allows for 'bulk' collection" when necessitated by operational circumstances and that this possibility does not "delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data."

		• Otherwise, generally yes - other US surveillance laws involve judicial oversight, controls, safeguards and redress mechanisms.
24.	***European Essential Guarantees for Surveillance Measures - Guarantee 2:*** *Is any such government access proportionate and limited to legitimate objectives (e.g. a public interest objective)?* *I.e. is the government's/public authorities' power to access the transferred personal data limited to what is necessary given the purpose and justified by the public interest at hand? Are the requirements indiscriminate for the given purpose and organising mass access on a generalized basis? (e.g. bulk surveillance)*	☐ Yes ☒ No ☐ Somewhat Please provide details: • The CJEU held in the Schrems II judgement that as far as FISA 702 and EO 12333 were concerned, limitations in US law on the protection of personal data are insufficiently circumscribed and not proportionate, because surveillance is not limited to what is strictly necessary. • Otherwise, generally yes, other US laws allowing USG access to personal data do not go beyond what is necessary and proportionate in a democratic society to safeguard important objectives also recognised in the EU.
25.	***European Essential Guarantees for Surveillance Measures - Guarantee 3:*** *Is any such government access subject to any independent judicial oversight mechanism(s)?* *I.e. is there any independent, effective and impartial mechanisms to approve and/or review government access and further use of the accessed data by public authorities (e.g. by a judge or another independent body)? Does it apply to access measures that are carried out in secret (if any)?*	☐ Yes ☒ No ☐ Somewhat Please provide details: • The CJEU held in the Schrems II judgement that the U.S. government's bulk surveillance activities under FISA 702 and EO 12333 were not subject to an independent and impartial oversight system. • However, FISA 702 is subject to general redress, as a party may challenge the applicability of FISA 702 and a USG request for the party's participation in the FISA 702 program under 50 U.S.C. § 1881a(j)). • Otherwise, generally yes.
26.	***European Essential Guarantees for Surveillance Measures - Guarantee 4:*** *In respect of any such government access, are there sufficient safeguard(s) for UK/EEA individuals? In particular consider:* *<u>(A) Effective legal remedies available to individuals and enforceable rights</u>* *Which legal remedies are available to the individuals whose personal data are accessed by authorities in the importing territory? Do individuals located in the UK/EEA have a right of redress in case of access by public authorities to the*	☐ Yes ☒ No ☐ Somewhat Please provide details: • **Individuals** - the CJEU held in the Schrems II judgement that European data subjects lack an adequate right of redress in connection with data that is accessed by the U.S. government under FISA 702 and EO 12333, as the latter do not confer rights which are enforceable against the US authorities (and, in particular, data subjects may lack standing under US law to challenge activities authorized under FISA 702 and

	transferred data? Can individuals effectively exercise their data protection rights (e.g. right of access, right to rectification and to erasure) in the importing territory? *(B) Effective legal remedies available to the data importer subject to government access* *Which legal remedies are available to the organisation based in the importing territory in the event of an access by authorities? Can it challenge the request and/or refuse to comply with the access request? Is there any public or known case law relating to a situation where a data importer in the importing territory opposes to a government access order or challenged the scope of such order and if so, what was the outcome?* *(C) Other relevant factors* *Is there anything else that is relevant to the risk of access in the importing territory (e.g. any reason or indication that authorities would have a special interest in accessing personal data originating from the UK/EEA)?*	EO 12333). Otherwise, generally yes to the extent the information is sought to be used against the individual in a criminal proceeding, although in some cases a defendant may lack standing or sufficient information to effectively seek redress. • **Data protection rights** - Unlike the EU, the US does not have a generally applicable law that provides individuals with data protection rights. Certain states (such as the California Consumer Privacy Act) do provide for such privacy right (e.g., right of access, right to rectification and erasure) but it would not be possible to exercise these rights at a federal law level. However, there are a number of sectoral laws at the federal level that grant individuals certain rights in respect of their personal information. • **Data importers' rights** - The data importer could take steps to challenge law enforcement or national security efforts to compel the data importer's production of data. Some types of process provide special procedures for challenging the process. EO 12333 does not provide the U.S. government a mechanism to compel parties to assist the government in carrying out its own surveillance efforts under EO 12333. However, the government's ability to meaningfully conduct surveillance under EO 12333 can be defeated by parties' use of strong encryption in transit. • **Case law** - As many of the activities of the FISC are conducted in secret, it is unclear how many challenges are brought against 702 FISA directives and whether these are successful. However, it appears that they are rare. Apart from direct challenges to FISA 702 directives, numerous US lawsuits have challenged the broader legality of FISA 702 under the US Constitution. The most notable are Clapper v Amnesty International USA (133 S. Ct 1138 (2013)) and Wikimedia Foundation v National Security Agency/Central Security Service (427 F. Supp. 3d 582 (D. Md. 2019)). These cases show the extreme difficulties organisations face in challenging FISA 702 without actual proof that the government targeted or accessed their specific communications. This point also played an important role in the Schrems II judgment, because it evidences the difficulty non-US persons would have in obtaining legal redress in the US.

		• **Other factors** - The type of foreign intelligence information sought by FISA 702 concerns US security interests and combatting potential attacks on the US (including through terrorism). Based on a whitepaper prepared by the US Department of Commerce, the Department of Justice and the Office of the Director of National Intelligence after the Schrems II judgment, many US businesses may find their surveillance interception risks are quite low or non-existent based on the fact that they do not process communications data and/or they only process data and communications relating to commercial products or services.
27.	*Has the importing territory entered into any international commitments regarding data protection, does it adhere to any international instrument on data protection standards that are legally binding (e.g. Convention 108, Convention 108+)?*	☒ Yes ☐ No ☐ Somewhat Please provide details: • The USA does not adhere to Convention 108. However, the United States adheres to international instruments on data protection standards, such as the Universal Declaration of Human Rights, and participates in the APEC Cross-Border Privacy Rules (CBPR) privacy certification program. • Additionally, although not a party to it, the United States has signed the UN Convention on the Rights of the Child, which incorporates the right to privacy.
28.	*Is the rule of law constitutionally recognised, are there laws that establish the rule of law in the importing territory? In particular, will governmental authorities abide by the importing territory's laws?*	☒ Yes ☐ No ☐ Somewhat Please provide details: • The US Constitution and its Bill of Rights enshrine a number of fundamental rights such as the right to petition the USG for redress, the right to due process of law and protection against unreasonable search and seizure by the government
29.	*Is the right to privacy/data protection recognised as a human right or fundamental right?*	☐ Yes ☐ No ☒ Somewhat Please provide details: • The US Constitution and its Bill of Rights do not enshrine an express right to privacy.

		• However, the First Amendment, the Third Amendment, the Fourth Amendment and the Fifth Amendment protect certain aspects of privacy, such as the protection against unreasonable search and seizure by the government. In addition, the US Supreme Court has established that the various guarantees within the Bill of Rights create "penumbras" (or zones) that establish a right to privacy.
30.	*Is there an independent supervisory authority that is responsible for:* • *ensuring and enforcing compliance with the data protection rules with adequate enforcement powers?* • *assisting and advising individuals in exercising their data protection rights?* *If that is the case, please briefly explain the role of this authority.*	☐ Yes ☐ No ☒ Somewhat Please provide details: • The US does not have a single independent supervisory authority responsible for ensuring and enforcing compliance with data protection rules or with assisting and advising individuals in the exercise of their data protection rights. • However, a variety of authorities at the state and federal level are responsible for rule-making and enforcing compliance with sectoral data protection rules.
31.	*Is there a comprehensive data protection framework applying to government authorities, including rules that restrict transfers of personal data to third countries to ensure that the personal data transferred continues to benefit from the level of data protection available in the importing territory?*	☐ Yes ☐ No ☒ Somewhat Please provide details: • The USA does not have comprehensive data protection law that applies to government authorities. • However, there are various laws that govern the collection, use and disclosure of personal information by US federal and state governments. For example, the Privacy Act establishes a code of fair information practices regarding the use of personal information by federal agencies. In the context of USG surveillance activities, there are a number of protections and safeguards that apply to USG collection and use of data in connection with security and surveillance. Some of these are found in the laws that authorize such activities, others in other legislation or directives. For example, PPD-28 is a presidential directive that imposes restrictions on signals intelligence activities by US intelligence agencies, including those conducted under FISA 702 and EO 12333. However, in the Schrems II judgment the CJEU held that the protections afforded by PPD-28 are

		not sufficient to ensure an adequate level of protection for personal data under the GDPR. • As regards, transfers, the USA does not have a generally applicable law (equivalent to Chapter V of the GDPR) that restricts the transfer of personal data to third countries.
32.	*Is the data importer and type of data to be transferred potentially within the scope of the importing territory's governmental security and surveillance powers? Please explain.*	☒ Yes ☐ No ☐ Somewhat Please provide details: • Every US-based cloud computing provider will qualify as a "remote computing service" or RCS, and therefore be an "electronic communications service provider" within the scope of s.702 FISA, like the data importer (and its US-based subprocessors). Accordingly, under powers including s.702 FISA and EO 12333 as further described above, USG authorities could obtain access to personal data processed by it, in a way that is contrary to its customers' processing instructions. • To date, however, the data importer has never received an order to disclose data to US government agencies. If it did, then it would have a contractual compulsion to notify EEA/UK controllers who export data to it pursuant to the EU Standard Contractual Clauses that it is unable to process personal data in accordance with their instructions, pursuant to Clause 5(a) of the SCCs. • Further, the data importer has implemented a government data access policy that would govern the data importer's response to any such order. This is described further below. • Further, data transmitted to or from the data importer via means of telecommunications infrastructure outside the US might also be accessed by USG pursuant to EO12333. However, the data importer would have no knowledge in practice whether this actually happens. EO 12333 can be and has been addressed through appropriate encryption in transit.
33.	*Beyond or in addition to those already described above, are there any practices in force of public authorities in the importing territory or any publicly reported*	☐ Yes ☒ No ☐ Somewhat

	precedents that, regardless of the content of its formal laws, involve unnecessary or disproportionate government authority access to transferred personal data or otherwise adversely affect its protection or the ability of UK/EEA individuals to exercise their data protection rights?	Please provide details: • Not aware of any beyond those already described above.
34.	*Are there any <u>other</u> applicable laws in the importing territory, beyond or in addition to those already described above, which could constitute an obstacle to its ability to comply with appropriate safeguards (e.g. its obligations under Standard Contractual Clauses or BCRs) and, in particular, ensure an essentially equivalent level of protection for the data transferred?* *E.g. are there any legal prohibitions on data importers informing exporters of a specific request for access to data received or restrictions on providing general information about requests for access to data received or the absence of requests received?*	☐ Yes ☒ No ☐ Somewhat Please provide details: • Not aware of any beyond those already described above.
35.	*Can the data importer confirm whether it has or has not received requests for access to transferred personal data from the importer's territory's government authorities in the past and that it is not prohibited from providing information about such requests or their absence?*	☒ Yes, the data importer confirms it has never received any such requests and is not prohibited from providing information about such requests or their absence. ☐ No, the data importer is prohibited from providing this information.
36.	*Is there good reason to believe that relevant and problematic legislation, that provides governmental security and surveillance powers and any extra-constitutional government access to transferred data, will not be applied, in practice, to the transferred data and/or data importer?* *This assessment should be, based on the above and also take into account the experience of others in the same sector and/or related to similar transferred personal data and additional sources of information that are relevant, objective, reliable, verifiable and publicly available?*	☒ Yes, there is good reason to believe that the legislation will not be applied, in practice, to the transferred data and/or this data importer. ☐ No, there is reason to believe that the legislation will be applied, in practice, to the transferred data and/or this data importer. Please provide details for this assessment: Please see the answer to question 35.

Local Country Risk Assessment and Rating

Based on the above, while the USA would otherwise be considered high risk, because there is good reason to believe that the relevant problematic legislation will not be applied, in practice, to the transferred data and/or data importer, these transfers may be permitted to continue. Nevertheless, additional safeguards have been taken to protect the transeferred data, as indicated in Part 4 below.

Adjusted Country Risk Rating	Low

Part 4: Identify the additional safeguards taken to protect the transferred data[1]		
Technical measures		
37.	***Encryption at rest**: Is the data importer storing encrypted data for backup or other purposes that do not require it to have access to data in the clear?* *(EDPB Supplementary Measures Guidance: Use Case 1)*	☒ Yes ☐ No If Yes, please confirm which (if any) of the following applies: ☒ The identity of the data importer is verified ☐ Encryption is applied before transmission ☒ The encryption algorithm, key length etc. are state of the art and robust against by public authorities' crypto-analysis, taking account of resources available to them ☒ The encryption strength and key length take account of the specific time period during which data confidentiality must be preserved ☒ The encryption algorithm is implemented correctly by properly maintained software without known vulnerabilities ☒ The software's conformity to the algorithm specification has been verified e.g. by certification ☒ Keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended data importer, and revoked) e.g. in accordance with NIST 800-57[2] ☐ Keys are under the sole control of the data exporter or an entity trusted by it in the EEA or in a jurisdiction offering essentially equivalent protection (e.g. adequate country)
38.	***Pseudonymisation before transfer**: Will the data be pseudonymised before transfer?*	

[1] This Part 4 only needs to be completed if personal data is being transferred to a non-adequate country that does not have essentially equivalent protection and the transfer is not in reliance on an Article 49 derogation.

[2] https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

	(EDPB Supplementary Measures Guidance: Use Case 2)	☐ Yes ☒ No If Yes, please confirm which (if any) of the following applies: ☐ The data been pseudonymised so that it can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group without the use of additional information ☐ The additional information is held only by the data exporter and kept separately in a Member State, or by an entity trusted by the data exporter in the EEA or an essentially equivalent jurisdiction (e.g. adequate country) ☐ Disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards ☐ The data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information ☐ The data exporter has established by thorough analysis of the data, taking into account any information that the public authorities of the importing territory may be expected to possess and use (e.g. through requests to other service providers or use of public information), that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information
39.	***Encryption in transit:*** *Is the data encrypted while transiting third countries without essentially-equivalent protection on its way to a data importer in a country whose public authorities can access data in transit?* *(EDPB Supplementary Measures Guidance: Use Case 3)*	☒ Yes ☐ No If Yes: ☒ Transport encryption is used with state of the art encryption protocols to provide effective protection against active and passive attacks with resources known to be available to the public authorities ☐ The data exporter and data importer have agreed on a trustworthy public-key certification authority or infrastructure ☒ Specific protective state-of-the-art measures are used against active and passive attacks on sending and receiving systems providing transport

		encryption, including tests for software vulnerabilities and possible backdoors ☐ Personal data is encrypted end-to-end on the application layer using state-of-the-art encryption methods ☒ The encryption algorithm and key length etc. conform to the state-of-the-art and can be considered robust against public authority cryptanalysis taking into account their resources ☒ The encryption strength and key length take account of the specific time period during which data confidentiality must be preserved ☒ The encryption algorithm is implemented correctly by properly maintained software without known vulnerabilities ☒ The software's conformity to the algorithm specification has been verified e.g. by certification ☒ Keys are reliably managed e.g. in accordance with NIST 800-57, by the data exporter or an entity trusted by exporter under a jurisdiction offering essentially equivalent protection.
40.	***Protected recipient:*** *Will the data be transferred to a data importer specifically protected by the importing territory's laws, e.g. under medical or legal confidentiality?* *(EDPB Supplementary Measures Guidance: Use Case 4)*	☐ Yes ☒ No If Yes: ☐ The importing territory's law exempts a resident data importer from potentially infringing access to data held by that data importer for the given purpose, e.g. by virtue of a duty to professional secrecy applying to the data importer, ☐ The exemption extends to all information in the possession of the data importer that may be used to circumvent protection of privileged information (keys, passwords, other credentials, etc.) ☐ The data importer does not engage a processor in a way that allows public authorities to access the data while held by the processor, nor does the data importer forward the data to another entity that is not protected, on the basis of Article 46 GDPR transfer tools

		☐ The personal data is end to end encrypted before transmission with a state of the art method guaranteeing that decryption will not be possible without knowledge of the key (end-to-end for the whole length of time the data needs to be protected ☐ The decryption key is in the sole custody of the protected data importer, and, possibly, the data exporter or another entity trusted by the data exporter located in the EEA or an essentially equivalent jurisdiction, and appropriately secured against unauthorised use or disclosure by state of the art technical and organisational measures ☐ The data exporter has reliably established that the intended key corresponds to the key held by the data importer
41.	***Split or multi-party processing:*** *Will the data importers be involved in secure multi-party computation ("**MPC**"), whereby two or more independent processors in different jurisdictions will process the data without the data content being disclosed to any of them, i.e. the data is split before transmission such that no part an individual processor receives suffices to reconstruct the personal data in whole or in part, with the data exporter receiving the processing results from each of the processors independently and merging them to produce a final result which may constitute personal or aggregated data?* *(EDPB Supplementary Measures Guidance: Use Case 5)*	☐ Yes ☒ No If Yes: ☐ The data is split into two or more parts each of which can no longer be interpreted or attributed to a specific data subject without the use of additional information ☐ Each part is transferred to a separate processor in a different jurisdiction ☐ The processors optionally process the data jointly, e.g. using secure multi-party computation, such that no information is revealed to any of them that they do not possess already ☐ The algorithm used for the shared computation is secure against active adversaries ☐ The data exporter has established by thorough analysis of the data, taking into account the missing pieces of information that public authorities of data importer countries may be expected to possess and use, that the parts transmitted to the processors cannot be attributed to an identified or identifiable natural person even if cross referenced with such information ☐ There is no evidence of collaboration between public authorities located in the respective processor jurisdictions which would allow them access to all sets of personal data held by the processors and enable them to

		reconstitute intelligible content where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects ☐ Public authorities of importing countries do not have the authority to access personal data held by processors in all jurisdictions concerned.
42.	***Transfer with access to data in the clear:*** *Will the data be transferred to a data importer processor in a third country that requires access to data in the clear to provide its service/perform its functions?* *(EDPB Supplementary Measures Guidance: Use Case 6)*	☒ Yes ☐ No Please give details: Please see the answer to Q3 above. [**Note**: *If Yes, and in practice the data importer territory's public authorities are empowered to access the unencrypted transferred data beyond what is necessary and proportionate in a democratic society, the EDPB's view is that no technical measures can prevent that access infringing on data subjects' rights.* *Note that the EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear*.]
43.	***Remote access to data:*** *Will the data be transferred (or direct access permitted to data) unencrypted without pseudonymisation because it is required in the clear in the data importer territory for business purposes? E.g. HR data or customer support.* *(EDPB Supplementary Measures Guidance: Use Case 7)*	☒ Yes ☐ No Please give details: Please see the answer to Q3 above. [**Note:** *If Yes, and in practice the data importer territory's public authorities are empowered to access the unencrypted transferred data beyond what is necessary and proportionate in a democratic society, the EDPB's view is that no technical measures can prevent that access infringing on data subjects' rights*.]
Contractual measures		
44.	*Does the contract contain terms requiring implementation of any of the specific technical measures set out above (as applicable)?*	☐ Encryption at rest ☐ Pseudonymisation before transfer ☐ Encryption in transit ☐ Protected recipient

		☐ Secure multi-party computation (MPC)
45.	*Does the contract contain contractual obligations providing for transparency regarding access to data by public authorities in the data importer territory? Tick any of the following that apply in the contract.*	☒ Requirement for the data importer to provide information on data importer territory's laws/regulations allowing public authority access to transferred data, particularly for intelligence, law enforcement, administrative and regulatory supervision, to best of the data importer's knowledge/belief based on its best efforts ☐ If no laws govern such access, requirement for the data importer to provide information and statistics from data importer's experience or reports from public sources on public authority access to transferred personal data in this type of situation (e.g. this regulatory area/sector; type of data importer) ☒ Information on measures taken by the data importer to prevent access to transferred data ☒ Sufficiently detailed information on all requests for access the data importer has received over a specified period of time (e.g. year), including requests received, data requested, requesting body, legal basis for disclosure, and to what extent it disclosed the data ☐ Details about whether and to what extent the data importer is legally prohibited from providing any of the information listed above ☐ An obligation on data importer to notify any changes to the above ☐ Certification by the data importer that (1) it has not purposefully created back doors or similar that could be used to access the system and/or personal data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) national law or government policy does not require it to create or maintain back doors or to facilitate access to personal data or systems or for it to hold or hand over the key (plus penalties/termination right for breach of this obligation, possibly compensation to data subjects) ☐ Audit/inspection right for the data exporter, including remote access to logs, to verify if data was disclosed to public authorities and under which conditions, e.g. by providing for short notice and mechanisms ensuring rapid intervention of inspection bodies and exporter's right to select them

		☐ Requirement for logs/audit trails to be tamper proof and regularly transmitted to the data exporter, distinguishing between normal business access and access under orders/requests? ☐ Even if data importer territory is essentially equivalent, obligation to inform exporter promptly of inability to comply with contract if situation changes e.g. changes in data importer territory's legislation/practice; with specific time limits/procedures for suspending transfers and/or terminating the contract and return/deletion of transferred data before authorities' access and if possible before the change Is implemented, and mechanism to authorise data importer to promptly secure or return data or delete/securely encrypt without awaiting instructions if a set threshold is met (with regular testing), and possibly monitoring/audit rights with penalties and right to suspend/terminate ☐ Warrant canary if data importer territory's law allows, i.e. an obligation on data importer to regularly publish (e.g. at least every 24 hours) a cryptographically signed message informing the data exporter that as of a certain date and time it has received no order etc to disclose personal data, with secure private key or multiple signatures needed or issue by a person outside the data importer territory
46.	*Does the contract contain obligations to take certain specific actions? Tick any of the following that apply in the contract.*	☒ Commitment to review, under data importer territory law, the legality of any order to disclose data, notably the scope of requesting public authority's powers, and to challenge the order if, after a careful assessment, data importer concludes there are grounds for challenge under data importer territory law, including seeking interim suspension of the order until the court decision, and obligation not to disclose requested data until required under applicable procedural rules and to provide the minimum amount of information permissible based on a reasonable interpretation of the order ☐ Commitment to inform the requesting public authority of the incompatibility of the order with the safeguards in the Article 46 GDPR transfer tool and the resulting conflict of obligation (which must have helpful legal effects in the data importer territory), and to notify as soon as possible the data exporter and/or the competent EEA supervisory authority, insofar as possible under data importer territory law.

		☐ Require that intelligible data transmitted for business purposes may be accessed only with express/implied agreement of the data exporter and/or data subject to a specific access (e.g. requests for voluntary disclosure) ☐ Oblige the data importer and/or the data exporter to notify promptly (or as soon as any national restrictions are lifted, with best efforts to seek waiver of prohibition to disclose) the data subject of a request or order, or of the data importer's inability to comply with the contract (to enable data subjects to seek information and redress, including compensation for the disclosure. ☐ Obligations on both data importer and data exporter to assist (or procure assistance to) the data subject to exercise rights in the data importer territory through ad hoc redress mechanisms (if the country provides for redress including against surveillance) and legal counselling.
Organisational measures		
47.	Are relevant internal policies, organisational methods, and/or standards applied or imposed on the data importer? Tick any of the following that apply.	☒ Adequate internal policies exist with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for formal or informal requests to access the data (especially for intragroup transfers), including appointment of a specific team (IT, data protection and privacy experts) to deal with requests that involve personal data transferred from the EEA; notification to senior legal and corporate management and to the data exporter upon receipt of such requests; procedural steps to challenge disproportionate or unlawful requests; and provision of transparent information to data subjects. ☒ Training is in place for personnel in charge of managing requests for access, periodically updated to reflect new legal developments in the importing territory and EEA, including on EU requirements as to access by public authorities to personal data, in particular Article 52 (1) Charter of Fundamental Rights, raising awareness of personnel by assessment of practical examples of public authorities' data access requests and by applying the Article 52(1) standard to the practical examples, taking into account data importer territory legislation and regulations applicable to the data importer (developed where possible in cooperation with the data exporter).

48.	Are there transparency and accountability measures regarding public authorities' access to data? Tick any of the following that apply.	☒ The data importer documents and records requests and responses provided to access requests (see Contractual measures above), including legal reasoning and actors involved (e.g. if the data exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.); and these will be made available to the data exporter. ☐ The data importer regularly publishes transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law.
49.	Has data importer implemented confidentiality, audit and escalation measures governing transfers of, and access to, data? Tick any of the following that apply.	☒ The data importer has in place strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures, focusing on data minimisation with technical measures to restrict access (it might not be necessary to transfer certain data e.g. restricting remote access to EEA data for support, or when service provision only requires transfer of a limited dataset and not the entire database). ☒ Development of best practices to appropriately and timely involve and provide access to information to the data protection officer, if any, and to legal and internal auditing services on matters related to international transfers of personal data, before the transfer is effected.
50.	Is there evidence of adoption of standards and best practices by the data importer? Tick any of the following that apply.	☒ The data importer has in place strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA) with due regard to the state of the art, in accordance with the risk of the categories of data processed.
51.	Has the data importer implemented any other measures? Tick any of the following that apply.	☒ The data importer has adopted and regularly reviews internal policies to assess suitability of implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection is maintained. ☒ The data importer has provided commitments not to engage in any onward transfer of the personal data within the same or other third countries, or suspend ongoing transfers, when an essentially equivalent level of protection cannot be guaranteed.

Part 5: Overall Risk Assessment		
Reviewer assessment		
52.	Please provide your overall conclusion of the risk of this transfer:	In view of the assessments of the data importer, the data importer territory, the nature of the data transferred and the appropriate safeguards implemented by the data importer, and in particular the lack of previous access requests and good reason to believe the relevant legislation will not be applied in practice to the data importer, the risk of proceeding with this transfer is low
53.	Please provide details of any risk mitigations measures recommended prior to transfer:	N/A. No further measures required at this stage – the position should be revisited on the next assessment date.
DPO assessment (if any)		
54.	Please provide the DPO's overall conclusion of the risk of this transfer:	In view of the assessments of the data importer, the data importer territory, the nature of the data transferred and the appropriate safeguards implemented by the data importer, and in particular the lack of previous access requests and good reason to believe the relevant legislation will not be applied in practice to the data importer, the risk of proceeding with this transfer is low
55.	Please provide details of any risk mitigations measures recommended by the DPO prior to transfer:	N/A

Document Control

Version History

Revision	Modified by	Date	Comments
1.0	Lianne Harcup	01.10.21	Template Created
2.0	Lianne Harcup	21.10.22	Review no changes implemented apart from review date change.
3.0	Lianne Harcup	14.06.23	Review no changes apart from assessment made.

Contacts

Name	Role	Email	Telephone
Lianne Harcup	Data Protection Officer - Europe	gdpr@trendmicro.com	+353 730 7000