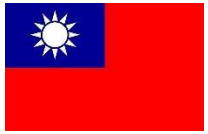

Trend Micro

Transfer Impact Assessment – Taiwan

Data exporting entity: Trend Micro US Incorporated ("data exporter")

Part 1: Know Your Transfers		
A. Assessment of the data importer		
1.	*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 Inc Taiwan
2.	*What does the data importer do?* *Provide details of the product or service they will provide.*	Provide technical product support services and deliver pattern solutions to threat escalations.
3.	*Where (in what country or countries) will the data importer process the data?*	Taiwan
4.	*Is the data importer a group company?*	X Yes ☐ ~~No~~ If no, is the data importer: ☐ A public authority

<table>
<tr><td></td><td></td><td>X A private enterprise (i.e. a company)
☐ A not-for-profit</td></tr>
<tr><td>5.</td><td>Why will the data importer process the personal data?
Please explain what processing activities the data importer will perform.</td><td>To provide support services

Customer information is used to confirm entitlement and license validity and contact information is used for follow-up activities for tech support activities.</td></tr>
<tr><td>6.</td><td>Why are these transfers necessary? Could the processing instead be conducted in the European Economic Area (EEA) (for EEA data) or UK (for UK data)?</td><td>Data that is stored in system (AWS/ Salesforce in US) is accessed by engineers in the Philippines to provide the support services as described in more detail above.</td></tr>
<tr><td>7.</td><td>Has a DPIA been conducted for the data importer's processing?
If no, why not?</td><td>☐ Yes, a DPIA has been conducted and is available at [give details].
X No, a DPIA has not been conducted because the processing is not "high risk" within the meaning of Art 35 GDPR)</td></tr>
<tr><td>8.</td><td>Will the data importer <u>onward transfer</u> the personal data to other third parties? If so, please complete the table to (i) identify all such third parties and their location; (ii) 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)?

Note: Both "transfer" and onward transfer" include remote access. Onward transfer can be to the same or another third country.</td><td>☐ Yes X No
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></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>9.</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>☐ N/A – no onward transfers
☐ Yes, TIAs have been conducted and are available at [give details].
☐ No, TIAs have not been conducted because [give details].</td></tr>
<tr><td colspan="3">B. Assessment of the data transferred</td></tr>
<tr><td>10.</td><td>What categories of data are being transferred?</td><td>Consumer: Customer name, social media username, email address, phone number, home/billing address, birthday, IP address
Corporate: contact information, company info, product info
CoreTech: company name</td></tr>
</table>

11.	*Does the data include communications contact information such as telephone numbers, email addresses or physical addresses?*	x Telephone numbers x Email addresses x Physical addresses

12.	*Does the data include telephone, email or other wire or electronic communications content?*	☐ Telephone content X Email content ☐ Other wire or electronic communications
13.	*Does the data include special categories of data?*	☐ ~~Yes~~ x 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
14.	*Does the data include data about criminal convictions and offences?*	☐ ~~Yes~~ x No If yes, please explain why: [Give details, if applicable]
15.	*Is the data otherwise inherently sensitive (e.g. banking data, social security data) or likely to be of interest to government security or surveillance authorities (e.g. social media data)?*	☐ ~~Yes~~ x No If yes, please explain why: [Give details, if applicable]
16.	*Will this be a 'one-off' transfer or an ongoing series of transfers?*	☐ ~~One-off~~ / X Ongoing

17.	*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 Approximate number of data subjects (if possible to estimate): Not possible to approximate as it depends on number of customers and queries.

Part 2: Identify the transfer tool relied upon

18.	*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~~ x No If Yes, please note that it is not necessary to complete the rest of this form.
19.	*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.*	X SCCs ☐ BCR ☐ Approved code/ certification – please specify which: [Give details, if applicable] ☐ Other – please specify: [Give details, if applicable]

20.	*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: [Give details, if applicable]

Part 3: Is the transfer tool relied upon effective in light of the circumstances of the transfer?		
21.	*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: • **The Communication Security and Surveillance Act ("CSSA")** stipulates different conditions and procedures of surveillance for (i) criminal investigations and (ii) national security. Said communications include (i) symbols, texts, images, sound and other types of information sent, stored, transmitted and/or received via telecommunications device/equipment; (ii) mail and letters; and (iii) speeches and conversations. <u>Surveillance for criminal investigation</u> If (a) there is sufficient evidence that the accused or suspect is involved in any of the criminal offences listed in Paragraph 1, Article 5 of the CSSA, which may severely endanger national security, economic order, or social order; (b) there is reasonable belief that the content of his/her communications is relevant to the case being investigated; and (c) it is difficult or there is no other method to collect or investigate evidence, the law enforcement authority may apply to the court for its issuance of a surveillance warrant. <u>Surveillance for gathering intelligence on national security</u> If it is necessary to conduct surveillance on the following communications in order to collect intelligence on foreign forces or hostile foreign forces so as to ensure national security, the head of the authority overseeing national intelligence may issue a surveillance warrant: (a) domestic communications of foreign forces, hostile foreign forces, and/or their agents; (b) cross-border communications of foreign forces, hostile foreign forces, and/or their agents; or (c) offshore communications of foreign forces, hostile foreign forces, and/or their agents. Nonetheless, if any of said persons has a registered permanent address within Taiwan, the issuance of surveillance warrant shall be reviewed and approved by the high court that has jurisdiction over the authority overseeing national intelligence; except in case of emergency.

		Surveillance period and the extension thereof Each period of surveillance for criminal investigation shall not exceed 30 days, while each period of surveillance for gathering intelligence on national security shall not exceed one year. If it is necessary for the surveillance to continue, specific reasons must be provided, and the extension request shall be filed no later than two days before the expiration date of the original surveillance period. Limitation on Processing The information gathered via surveillance of communications shall not be provided to other agencies, groups or individuals or used for any purpose other than criminal investigation or national security. Moreover, all the safekeeping, use and destruction of the information gathered via surveillance of communications shall be traceably recorded, and such records shall be linked with the Communications Surveillance Management System of the Taiwan High Court. • **Pursuant to the Code of Criminal Procedure ("CCP")**, the person, property, electronic record, dwelling, or other premises of a third party may be searched when the court has "probable cause" to believe that the property or electronic record subject to seizure is there. Hence, the law enforcement authority may apply to the court for its issuance of a warrant to search the data importer's premises and property and seize such property. In principle, all searches and seizure must be conducted based on "probable cause" and with a warrant issued by the court. In case of emergency (e.g., any evidence will be forged, altered, destructed or concealed within 24 hours unless a search is undertaken), the law enforcement authority may initiate a search without a warrant, provided that it must report to the court the same within three days thereafter. • **Telecom operators' obligations to assist the law enforcement authority in conducting lawful interception and provide "communications records" and/or "user data/communications user data"**

		Under Taiwan law, telecom operators may be required to assist the law enforcement authority in conducting lawful interception and provide the law enforcement authority with "communications records" and/or "user data/communications user data". *Telecom Operators' Obligations of Assisting Surveillance by the Government under Telecommunications Act (Old Law)* The Telecommunications Act ("**Old Law**") was the main source of law for the telecom sector in Taiwan until the Telecommunications Management Act ("**New Law**") took effect on July 1, 2020. Nonetheless, there is a sunset clause granting a three-year transition period from July 1, 2020 to June 30, 2023. During the three-year transition period, existing telecom operators yet to file an application with the National Communications Commission (NCC) for (i) cancelling their telecom licences granted under the Old Law; or (ii) registering as a telecom operator pursuant to the New Law will continue to be regulated by the NCC in accordance with the Old Law. Under the Old Law, telecom operators are divided into two categories: Type I telecom operators and Type II telecom operators. Pursuant to Article 11 of the Old Law, Type I telecom operators refer to enterprises that install telecommunications line facilities and equipment to provide telecom services. Type II telecom operators are telecom operators other than any Type I telecom operator. Type I telecom operators are generally perceived as "facility-based" telecom carriers, while Type II telecom operators are generally perceived as "service-based" telecom carriers. Under the Old Law, both Type I and Type II telecom operators are required to obtain a telecom license from the NCC. Nonetheless, the NCC holds the view that purely Internet-based services should not be deemed as telecom services and thus do not require a telecom license. 1. Interception of Communications Under the Old Law, only Type I telecom operators and certain Type II telecom operators, namely (i) E.164 internet telephony service providers; (ii) non-E.164 internet telephony service providers (excluding voice communications over the Internet without using

		VoIP gateway); (iii) voice simple resale service providers; and (iv) Internet access service providers ("**IASPs**") additionally providing e-mail services, are obligated to assist the law enforcement authority in conducting lawful interception. 2. Communications Records and User Data Article 7 of the Old Law requires telecom operators to provide the law enforcement authority with "communications records" and/or "user data" when the law enforcement authority raises such request pursuant to the relevant applicable laws and regulations. Pursuant to Article 2 of the Old Law, "communications records" refer to the information generated by a telecom system concerning use of a telecom service, including sending and receiving parties' telecom numbers, date of communications, beginning/ending times of communications, and so on, to the extent that the technology of the telecom system and equipment allows. The rulings issued by the NCC further require that Type I telecom operators maintain the following types of "communications records": a. Local calls for the past three months; b. International calls and local long-distance calls for the past six months; and c. Mobile phone calls for the past six months. As for Type II telecom operators, internet telephony service providers, voice simple resale service providers and MVNOs are required to maintain phone calls for the past six months, while IASPs are subject to the following retention requirements: a. Dial-up Internet access subscribers' identification accounts, dates of communications, and on-line/off-line times shall be retained for at least six months. b. ADSL subscribers' identification accounts, dates of communications, and on-line/off-line times shall be retained for at least three months.

		c. Cable modem subscribers' identification accounts, dates of communications, and on-line/off-line times shall be retained for at least three months. d. Source IP addresses of the content posted on bulletin boards, picture forums, or news discussion groups and the system time at which such content was posted shall be retained for at least three months. e. Source IP addresses from which an IASP receives applications for a free e-mail address or web page and the system time at which the IASP receives such applications shall be retained for at least six months. f. E-mail correspondence shall be retained for at least one month. Unlike the retention obligations imposed on Type I telecom operators which are limited to "phone calls", those imposed on Type II telecom operators (to be specific, IASPs) may cover IP address related information. On the other hand, pursuant to the rulings issued by the NCC, "user data" under the Old Law refers to a user's name, national ID card number, mailing address, and telecom number, and such data is limited to the information that a user submitted to a telecom operator when he/she applied for (subscribed to) such telecom operator's services. *Telecom Operators' Obligations of Assisting Surveillance by the Government under Telecommunications Management Act (New Law)* Under the New Law, telecom operators are no longer divided into Type I or Type II telecom operators, and the regulatory regime has been shifted to voluntary registration. Only those intending to provide telecom services by using certain resources (such as radio frequencies or telecom numbers allocated by the NCC) or rights (e.g., mandatorily requiring other registered telecom operators to negotiate an interconnection agreement) conferred by the New Law need to register itself with the NCC as a telecom operator. Moreover, pursuant to Paragraph 4, Article 9 of the New Law, only (i) registered telecom operators; and (ii) enterprises establishing a public telecom network and designated by the competent

		authority in charge of communications surveillance (i.e., the National Police Agency) need to assist the law enforcement authority in conducting lawful interception and provide the law enforcement authority with "communications records" and/or "communications user data". On the other hand, Paragraph 1, Article 9 of the New Law and the rulings issued by the NCC require registered telecom operators to keep users' "communications records" for at least one year. Pursuant to Paragraph 2, Article 9 of the New Law, said "communications records" refer to the information generated by a public telecom network concerning use of a telecom service, including sending and receiving parties' telecom numbers, time of communications, length of usage, address, type of service, e-mail, location data, and so on, to the extent that the technology of the public telecom network allows. As for "communications user data", pursuant to the CSSA, such data refer to a telecom service user's name, identification document number, mailing address, telecom number, and other information that such user submitted to a telecom operator when he/she/it applied for (subscribed to) such telecom operator's services. • **Pursuant to Article 22 of the Personal Data Protection Act ("PDPA")**, both the local government authorities and central competent authorities in charge of the relevant industry sectors have the power to carry out audits and inspections on non-government agencies. In order to audit and inspect any non-compliance, they may: (i) access the premises of non-government agencies; (ii) require information; and (iii) detain or copy personal data or personal information files that can be confiscated or submitted as evidence. If a non-government agency is found in violation of the PDPA, said authorities may impose an administrative fine and take any of the following actions: (i) prohibit the non-government agency from collecting, processing or using the personal data; (ii) demand the deletion of the personal information files already processed; (iii) confiscate or destroy the personal data illegally collected; and (iv) publicise the violation case, the name of the non-government agency, and the name of the person in charge. In addition to the PDPA, in order to audit and inspect any non-compliance, the Fair Trade Act ("**FTA**") and the Multi-Level Marketing Supervision Act ("**MLM Act**") also allow the Fair Trade

		Commission (FTC) to carry out audits and inspections and detain things that can be submitted as evidence.
22.	***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: Please refer to our response to Question 21. All such government access is based on laws and regulations with clear, precise and accessible scope and application.
23.	***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: All Taiwan government authorities must observe the principle of proportionality when exercising their powers. Moreover, Article 5 of the PDPA stipulates that the collection, processing, and use of personal data shall not go beyond the necessary extent of the purpose(s) for which the data was collected, and must be reasonably and justifiably related to such purpose(s), regardless of government agencies or non-government agencies. According to the rulings issued by the Ministry of Justice (MOJ), "pre-determined and comprehensive" collection of personal data (e.g., mass access on a generalized basis) would be considered contradictory to the principle of proportionality. The only exception may be the recent adoption of innovative technology to trace individuals for the purpose of prevention of spread of COVID-19, which is subject to hot debate in Taiwan.
24.	***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: There is no regular judicial review with regard to government access to personal data. Also, there is no other impartial mechanism to approve and/or review government access to data. Government access will only be subject to judicial review when a lawsuit is brought by a data subject. Said judicial review also applies to access measures that are carried out in secret. Moreover, targets of surveillance are entitled to initiate an interlocutory or quasi-interlocutory procedure for the review of communications surveillance

		with the courts. We are not aware of any lawsuit being brought by an entity in the capacity of a data importer. Such cases are rarely seen.
25.	***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:* *(A) Effective legal remedies available to individuals and enforceable rights* *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 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)?*	☒ Yes ☐ No ☐ Somewhat Please provide details: *(A) Effective legal remedies available to individuals* Data subjects may file an administrative appeal against such government access with their superior authorities and seek judicial remedies from administrative courts. The aforesaid legal remedies are also available to foreigners. Nonetheless, state compensation is offered to foreigners based on the principle of reciprocity. Pursuant to Article 3 of the PDPA, a data subject has the following rights in relation to his/her personal data: (i) can access the personal data to check and review such; (ii) can obtain a copy of the personal data; (iii) can supplement or correct the personal data; (iv) can request the cessation of collection, processing, or use of the personal data; and (v) can request deletion of the personal data. A foreigner may also exercise such data subject rights in Taiwan. *(B) Effective legal remedies available to the data importer* The data importer may also file an administrative appeal against such access with their superior authorities and seek judicial remedies from administrative courts. *(C) Other relevant factors* Not aware of any beyond those already described above.
26.	*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: Taiwan has not entered into any international commitment or treaty regarding data protection. However, Taiwan has been recognized as a member of the Cross Border Privacy Rules System (CBPR) established by APEC.
27.	*Is the rule of law constitutionally recognised, are there laws that establish the rule of law in the importing territory?*	☒ Yes ☐ No ☐ Somewhat Please provide details:

		Pursuant to Article 23 of the Constitution, the government must exercise its power in accordance with the law. The principle of rule of law has also been recognized by the Grand Justices of Constitutional Court as a basic principle of the Constitution.
28.	*Is the right to privacy/data protection recognised as a human right or fundamental right?*	☒ Yes ☐ No ☐ Somewhat Please provide details: According to Judicial Yuan Interpretation No. 603 made by the Grand Justices of Constitutional Court, both the right to privacy and the right to informational self-determination, which is the basis of information privacy, are constitutional rights despite not being expressly stipulated in the Constitution.
29.	*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: Currently, there is no independent authority dedicated to personal data protection in Taiwan. The enforcement of the PDPA is administered by the local government authorities and central competent authorities in charge of the relevant industry sectors.
30.	*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: Most of the requirements under the PDPA also apply to government agencies, such as notification and data security. Nonetheless, only non-government agencies may be imposed with restrictions on cross-border transfer of personal data. Under the PDPA, cross-border transfer of personal data is, in principle, permitted. Nonetheless, under the authorization of Article 21 of the PDPA, the central competent authorities in charge of the relevant industry sectors may impose restrictions on cross-border transfer of personal data by non-government agencies under their charge if (i) the transfer would prejudice any material national interest; (ii) the transfer is prohibited or restricted under an international treaty or agreement; (iii) the country to which the personal data is to be transferred does not afford sound legal protection of personal data,

		thereby affecting the rights or interests of the data subjects; or (iv) the purpose of the transfer is to evade restrictions under the PDPA. In addition, the lawful grounds for a government agency to collect, process and use personal data are general, broad, and more flexible as compared to those for a non-government agency.
31.	*Is the data importer potentially within the scope of the importing territory's governmental security and surveillance powers? Please explain.*	☒ Yes ☐ No ☐ Somewhat Please provide details: Every person located in Taiwan, including the data importer, falls within the scope of the Taiwan government's governmental security and surveillance powers as described above. Nonetheless, as explained above, only certain telecom operators have the obligations to assist the law enforcement authority in conducting lawful interception and provide the law enforcement authority with "communications records" and/or "user data/communications user data". Trend Micro Taiwan would not be considered a "telecom operator" and therefore is not in scope of these obligations.
32.	*In terms of the practical application of these laws, are there any practices in force of public authorities in the importing territory or any publicly reported precedents that, regardless of the content of its formal laws, involve unnecessary or disproportionate public 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, or conversely ?*	☐ Yes ☒ No ☐ Somewhat Please provide details: Not aware of any beyond those already described above.
33.	*Is the data importer aware of any <u>other</u> applicable laws in the importing territory 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 except for the general confidentiality obligation with regard to the criminal investigation conducted a by a prosecutor.
34.	*Can the data importer confirm whether it has or has not received requests for access to data from public 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 received 0 requests in the past year and is not prohibited from providing information about such requests or their absence.

		☐ No, the data importer is prohibited from providing this information.
35.	*Is there good reason to believe that relevant and problematic legislation 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?*	X Yes, there is no reason to believe that the legislation will 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: Not aware of any beyond those already described above.

Part 4: Identify the additional safeguards taken to protect the transferred data[1]		
	Technical measures	
36	***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.

[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

		adequate country)
37	***Pseudonymisation before transfer**: Will the data be pseudonymised before transfer?* *(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
38	***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.
39	***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
40	***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?*	☐ 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

	(EDPB Supplementary Measures Guidance: Use Case 5)	☐ 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.
41	***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: [Give details] [**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*.]
42	***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: [Give details] Support case handling process/systems will not have access to the data except for the customer's email address which will only be accessed by system when the support team are replying to provide the analysis result of the case to the submitter. [**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		
43	*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)
44	*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
45	*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		

46	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).
47	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.
48	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.

49	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.
50	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		
51.	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
52.	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)		
53.	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 data transferred and the appropriate safeguards implemented by the data importer, the risk of proceeding with this transfer is low risk.
54.	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	03.02.22	Template Created
2.0	Lianne Harcup	14.06.23	Review no changes implemented apart from assessment made.

Contacts

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