TravelPerk International Data Transfers Whitepaper

TravelPerk

Table of Contents

About this document

Introduction

TravelPerk is committed to protecting our customers' privacy, which includes the security of the personal data we handle when providing platform services.

This document:

- summarises how our customers can use TravelPerk to transfer personal data outside the European Union (**EU**) or the European Economic Area (**EEA**) in compliance with EU law by relying on our industry-leading contractual, technical and organisational frameworks and safeguards.

- helps customers perform their own transfer impact assessments with regard to the use of TravelPerk services.

- provides customers and users with answers to some frequently asked questions regarding TravelPerk's data transfer practices in light of the ruling on the Case C-311/18 issued by the Court of Justice of the European Union (**CJEU**) on 16 July 2020, known as the "Schrems II" ruling. (A summary of the Schrems II ruling can be found in Appendix 1).

- explains the measures adopted by TravelPerk to ensure that an equivalent level of protection exists for personal data that, in connection with the use of TravelPerk services, is transferred out of the EEA, Switzerland and the UK to a country that has not been recognised by the European Commission (or the UK Government, as applicable) as ensuring adequate level protection for personal data (each a **Third Country**).

- provides an overview of the assurances made by TravelPerk to protect its customers' data from inappropriate disclosure to law enforcement and intelligence agencies.

Executive Summary

The process we follow every time we need to share customer's data with a vendor located in a Third Country is:

- We identify and map all our **Restricted Transfers** (i.e. any transfers of data to Third Countries).

- We require potential vendors to complete a thorough privacy questionnaire assessed by our Privacy team.

- We enter into a data processing agreement with the vendor, which sets out the same or equivalent data protection obligations as those set out in the DPA with our customers.

- We put the 2021 EU SCCs in place with every vendor processing personal data in Third Countries.
- We assess the laws of the vendor's country of storage, with special emphasis on the United States.
- We identify and adopt any additional safeguards and procedural steps needed to bring the level of protection of the data transferred up to EU standards.
- We re-evaluate our assessments periodically to make sure that the international transfers remain secure over time.

We value your feedback

We're happy to respond to any questions you may have on this document, or on our data transfer processes more generally.

Reach out to our Privacy team by contacting us at personaldata@travelperk.com.

TravelPerk's approach to International Data Transfers

Sharing our approach to international data transfers with our customers is an essential part of an overall privacy program to identify privacy risks, document compliance with applicable laws and internal policies, and build customer trust through transparency.

This section is intended to help customers perform the six steps of the EDPB Transfer Impact Assessment. You can find out more about the EDPB and its recommendations in Appendix 1.

Step 1: Identify international data transfers

TravelPerk operates on Amazon Web Services servers located in Ireland, with a fallback site at AWS Germany. Most of the sub-processors we engage for the provision of our services, as well as travel service providers acting as independent controllers, are also based in the EU or in countries that afford an adequate level of protection of personal data according to the European Commission (**Adequate Countries**).

We choose our vendors very carefully after performing thorough "Know-Your-Vendor" assessments. You can find out more about the assessments we undertake in Appendix 2. We prioritise the engagement of vendors located (or which store and process personal data) within the EU or in Adequate Countries.

Still, some of our vendors are located in Third Countries. The locations from which their services may be provided and a description of their processing activities are set out in the Data Processing Agreement (the **DPA**) we enter into with our customers, as well as in TravelPerk's sub-processors list.

The categories of Personal Data that may be transferred to our non-EEA sub-processors depend on the nature of the services provided by those vendors and the categories of personal data submitted to the TravelPerk services by the customer.

Step 2: Identify data transfer mechanisms

TravelPerk has a data processing agreement in place with all sub-processors we engage for the provision of our services. As mandated by the GDPR, essentially equivalent obligations as set out in the DPA between the customer and TravelPerk are imposed on TravelPerk's sub-processors, which are required in particular to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.

Should a sub-processor fail to fulfil its data protection obligations, TravelPerk remains fully liable to the customer for the performance of the sub-processor's obligations.

As regards those sub-processors located in Third Countries, our DPA contains the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (**EU SCCs**). The execution of the EU SCCs between TravelPerk and its sub-processors is deemed a legal contract entered into between contracting parties who are transferring personal data to Third Countries.

As further described in our DPA, transfers of customers' personal data to third parties may occur not only to sub-processors but also to certain vendors acting as independent controllers - particularly, travel service providers such as airlines, railway and taxi companies or hotels which are responsible for providing transportation or accommodation services to the travellers. To the extent that those travel service providers determine the means and purposes of the processing of personal data, they do so in a controller capacity.

Transfers of customer's personal data from TravelPerk to travel service providers located in Third Countries shall also be deemed an international data transfer, and as such, appropriate safeguards and the relevant data transfer mechanisms shall be put in place. In order to comply with such obligation, TravelPerk executes the relevant SCC modules (Module 1 Controller to Controller or Module 4 Processor to Controller, as applicable) with all travel service providers.

Step 3: Assess the laws or practices of Third Countries

This section describes possible privacy risks with regard to potential inappropriate disclosure to foreign law enforcement and intelligence agencies after the personal data gets transferred to Third Countries.

TravelPerk is not subject to regulations that may entail inappropriate disclosure to law enforcement and intelligence agencies in breach of the GDPR. Thus, this section will focus on such risks to the extent they may exist in countries where our sub-processors are located, with special reference to the United States.

As indicated in TravelPerk's sub-processors list, most of our non-EEA sub-processors are located in the United States. The Schrems II ruling highlighted the concerns about US intelligence agencies' access to EU and UK individuals' personal data. To address such concerns, we have set out specific processes and internal policies to make sure that any Restricted Transfer to the United States is carried out safely and in full compliance with EU data protection standards.

As a first step, we have assessed the specific US laws and practices that might compromise the effectiveness of the EU SCCs we have in place with our US vendors due to a potential access to customer data by US public authorities. Our attention has been drawn to the following laws:

FISA Section 702

Section 702 of the Foreign Intelligence Surveillance Act (**FISA Section 702**) sets forth processes and conditions for US intelligence agencies to lawfully collect information

relating to non-US individuals who are reasonably believed to be located outside the US if a significant purpose of such collection is to acquire foreign intelligence information and the source of the information is a US-based electronic communication service provider (**ECSPs**).

FISA Section 702 authorises "upstream" and "downstream" collection:

- Upstream collection authorises US authorities to collect communications as they travel over the Internet backbone.
- Downstream collection authorises US authorities to collect targeted data directly from ECSPs based in the US.

As further described below, we have set up processes to proactively assess whether and to what extent our vendors may be considered as an ECSP under FISA Section 702 and compelled to respond to US targeted requests for customer data. Our contracts with vendors include obligations for them to carefully review the lawfulness of any disclosure request they may receive, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if there are legal grounds to do so.

Executive Order 12333

Executive Order 12333 (**EO 12333**) authorises and governs surveillance activities by US intelligence agencies. As the CJEU noted, the primary concern regarding EO 12333 is the US government's ability to collect personal data while it is in transit to the US by intercepting data travelling over transatlantic cables. Personal data can effectively be protected from this type of interception through security measures such as **encryption**.

TravelPerk addresses this risk by encrypting Personal Data and only transferring data that is subject to strong protection. Please see our Security Whitepaper for more information about these measures.

EO 12333 does not grant the US government the ability to compel companies to provide assistance with such interceptions but our assessment of US vendors is aimed at ensuring that they will not do so voluntarily. Our priority is to only engage vendors that will not assist with government interception of customer data and cannot be ordered to take any action to facilitate such bulk surveillance.

CLOUD Act

The US Clarifying Lawful Overseas Use of Data Act (**CLOUD Act**) enacted in 2018, determines that US law enforcement authorities may request personal data from US-based technology companies when there is a suspicion of a crime by issuing warrants or court orders, regardless of the location of the data. Physical location of data is not the deciding factor but whether the recipient of a request has "possession, custody, or control" of the data.

A US service provider could be compelled to disclose any information related to a customer within the provider's possession regardless of whether such communication, record, or other information is located within or outside of the United States. Consequently, US authorities could be able to access and process large quantities of personal data belonging to EU citizens.

The CLOUD Act specifically contemplates court orders or warrants requiring the transfer of personal data to the United States even if the country of storage and the US don't have a Mutual Legal Assistance Treaty (**MLAT**). However, the EDPB concluded that "*service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests*." Pursuant to article 48 GDPR, court orders requesting the transfer or disclosure of personal data outside the EU are only acceptable if based on an international agreement, such as a MLAT. Other legal bases are also not acceptable under EU law for such requests.

The CLOUD Act also established certain safeguards to the companies, including allowing them to challenge any disclosure requests that conflict with the laws of another country. Accordingly, TravelPerk's assessment of our US vendors is aimed at ascertaining to what extent they may be compelled to respond to such requests for customer data. If one of our vendors is subject to the CLOUD Act, we impose contractual obligations to carefully review any request they may receive to:

- verify if it is lawful and appropriate, including with respect to the data sought and relevant jurisdiction, and
- challenge the request in accordance with GDPR principles and contractual commitments on government access requests, as per articles 14 and 15 of the EU SCCs, if appropriate.

Steps 4 to 6: Adoption of supplementary measures, necessary procedural steps and re-evaluation

This section summarises the various contractual, technical and organisational measures put in place by TravelPerk to ensure that customer personal data gets lawfully transferred to suppliers located in Third Countries.

Contractual safeguards

EU Standard Contractual Clauses

TravelPerk enters into the relevant EU SCCs and the applicable Modules with all processors and sub-processors, as well as with any other vendors in Third Countries acting as independent controllers, to the extent any personal data needs to be transferred to them. The 2021 EU SCCs were specifically drafted by the European Commission and approved by all EU member states after the Schrems II ruling in order to ensure appropriate data protection safeguards for international data transfers.

Additional contractual commitments

The EU Commission encourages controllers and processors to provide additional safeguards for transferring personal data overseas with supplementary contractual commitments that afford a level of protection essentially equivalent to EU standards.

TravelPerk conducts a thorough assessment of all our vendors in order to determine the effectiveness of the EU SCCs in each particular case. Based on the assessment results, we direct such vendors to incorporate additional contractual commitments to the relevant DPA. Our focus is both on the security measures implemented by the vendor and on specific safeguards to prevent or mitigate the risks of any requests for disclosure of personal data to public or authorities or law enforcement in the vendor's country (**Request**), especially in the US.

Depending on the case, we request our vendors to comply with some additional contractual commitments if they receive such Requests:

- To inform the requesting authority of the incompatibility of the Request with the safeguards contained in the EU SCCs and the resulting conflict of obligations for the vendor.

- To promptly notify TravelPerk of any received Request. Such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided to the authority.

- If a vendor is legally prohibited from notifying TravelPerk about the Request, it should use its best efforts to obtain a waiver of the prohibition, and communicate as much information as soon as the waiver is granted. The vendor should document its best efforts in relation to obtaining a waiver and demonstrate them upon our request.

- To review the legality of the Request under the applicable laws, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the Request if, after a careful assessment, it concludes that there are grounds under the applicable laws to consider that the Request is unlawful.

- To provide the minimum amount of information possible when responding to a Request.

- To implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data.

- To refrain from creating any back doors or similar programming that could be used to access the systems and/or personal data.

Technical safeguards

TravelPerk is committed to providing a robust security and privacy program that carefully considers data protection matters across our services. We offer industry leading technical measures to protect personal data against unauthorised access, as further described in this section.

We provide an overview of the standard security controls applicable to our services in our Security White Paper. Our comprehensive set of security controls protect data whilst in transmission within the cloud and at endpoint. Not only is data encrypted at rest and in transit, we also practice pseudonymisation and employ firewalls on our user platform and our network.

Organisational safeguards

TravelPerk has a number of organisational safeguards in place to protect personal data we process. It ensures that the contractual commitments described above are put into practice. This goal is achieved by implementing organisational safeguards such as:

- Policies and procedures to govern data protection best practice and to allow a privacy culture to be standardised across TravelPerk. This includes Data Protection, Global Retention, Information Security, Acceptable Use policies, as well as Data Breach and Data Subject Rights Request procedures;

- Regular reviews of security controls of our third parties to ensure they are effective. One of these is to send out Transfer Impact Assessments to our sub-processors to ensure adequate protection of data when transmitted. Additionally, we monitor our third-party vendors' security posture;

- Continually review the flow of customer data and make sure our compliance documentation is up to date such as our records of processing register.

- Having a dedicated Privacy Team driving a privacy culture within TravelPerk with a Data Protection Officer.

Appendix 1

The CJEU "Schrems II" Ruling

The Schrems II ruling is a reminder that the protection granted to personal data in the EEA must travel with the data wherever it goes. The CJEU clarifies that the level of protection in third countries does not need to be identical to that guaranteed within the EEA but essentially equivalent. From this perspective, Standard Contractual Clauses and Binding Corporate Rules remain valid contractual transfer tools to ensure an essentially equivalent level of protection for personal data transferred to countries considered by the European Commission as not providing an adequate level of data protection in the local regulations (**Third Countries**).

Controllers or processors acting as exporters are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country compromises the effectiveness of the appropriate safeguards contained in the transfer tools mentioned on Article 46 GDPR. If the verification concludes that the effectiveness of the GDPR appropriate safeguards is indeed compromised, the CJEU still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law.

The EDPB Recommendations

The European Data Protection Board (EDPB) adopted its Recommendations 01/2020 (version 2.0 adopted on 18 June 2021) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB Recommendations).

The EDPB adopted the EDPB Recommendations to help exporters with the complex task of assessing Restricted Transfers and identifying appropriate supplementary measures where needed. The EDPB Recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures they may put in place to carry out safe Restricted Transfers.

The six steps outlined by the EDPB - which are reflected in how TravelPerk protects personal data, as summarised in the main part of this white paper - are as follows:

(1) Know your transfers: Map all transfers of personal data to Non-adequate Countries to ensure that it is afforded an essentially equivalent level of protection wherever it is processed. Exporters must also verify that the data they transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

(2) Verify the transfer tool(s) on which the transfer relies: If the EU Commission has already declared the country, region or sector to which the data is being transferred as adequate through one of its adequacy decisions, exporters will

not need to take any further steps other than monitoring that the adequacy decision remains valid. In the absence of an adequacy decision, exporters need to rely on one of the transfer tools listed under Article 46 GDPR, or, only in some cases, on one of the derogations provided for in Article 49 GDPR.

(3) Assess Third Country's laws: Exporters must assess whether anything in the law and/or practices in force of the Third Country may impinge on the effectiveness of the appropriate safeguards of the transfer tools they are relying on. Such assessment should be focused on Third Country legislation that is relevant to the transfer and the Article 46 GDPR transfer tool the exporter is relying on. Examining these practices will be especially relevant for the exporter's assessment where:

(i) Third Country's legislation formally meets EU standards but is manifestly not enforced by the local authorities;

(ii) the lack of legislation in the third country allows the importer to carry out practices that are incompatible with the commitments set out in the transfer tool agreed with the exporter; and

(iii) the transferred data and/or the importer fall or might fall within the scope of problematic legislation (i.e. applicable laws that compromise the transfer tool's contractual guarantee of an essentially equivalent level of protection and don't meet EU standards on fundamental rights, necessity and proportionality).

(4) Identify and adopt supplementary measures: if the exporter's assessment reveals that the Third Country legislation and/or practices limits the effectiveness of the Article 46 GDPR transfer tool that is being relied upon in the relationship with the importer, importer and exporter should implement the applicable supplementary measures to level up the protection of the data transferred up to the EU-equivalent standards. The EDPB Recommendations contain a non-exhaustive list of examples of supplementary measures with some required effectiveness conditions.

(5) Adopt necessary procedural steps: depending on the Article 46 GDPR transfer tool used, the adoption of supplementary measures may require certain formal procedural steps (e.g. ensuring that any supplementary measures put in place do not contradict the EU Standard Contractual Clauses).

(6) Re-evaluate: the level of protection afforded to the personal data transferred to Third Countries needs to be re-evaluated at appropriate intervals, in light of any regulatory or practical developments that may affect it. The principle of accountability requires continuous vigilance of the level of protection of personal data.

Appendix 2

Assessment of TravelPerk (sub)processors

TravelPerk is committed to ensuring that any Restricted Transfers are conducted safely. We put that into practice by embedding a robust privacy due diligence into our third party management process.

Every potential vendor of TravelPerk processing personal data in a Third Country is required to respond to a detailed questionnaire addressing data protection concerns. The questions range from:

- implementation of robust personal data security measures
- internal data protection policies
- data subject requests response policy
- data breach prevention
- international data transfers and onward transfers mechanisms
- any additional safeguards to guarantee the effectiveness of such measures, especially in relation to potential disclosure requests from local public authorities and law enforcement.

Our Privacy team evaluates vendor's responses and assesses the potential privacy risk. Where we have any concerns that the personal data may not be protected enough against the disclosure to public authorities and law enforcement, the vendor is required to implement additional safeguards before accessing our data.

For the sake of transparency, the following sections contain the **questions sent by TravelPerk to our potential vendors** to assess the security of Restricted Transfers:

All vendors

Data storage

- Where is the data processed on behalf of TravelPerk hosted?
- Is it conceivable that all data processed on behalf of TravelPerk will be hosted exclusively within the EEA, with no access, including for customer support, from outside the EEA and in particular from the United States?

Onward transfers

- Do you transfer data processed on behalf of TravelPerk to sub-processors (including affiliates) located in countries outside the EEA?
- Have you documented the countries and international organisations to which personal data can possibly be transferred?

- Have you adopted a procedure to inform/ask TravelPerk about any new sub-processor (before use)?
- What transfer mechanisms do you rely on for onward transfers to your sub-processors outside the EEA to ensure the data is adequately protected?
- Do you have the current EU SCCs in place with all your sub-processors? [SCCs approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021]
- Do you ensure that all your sub-processors provide an adequate level of protection to the personal data processed on behalf of TravelPerk, essentially equivalent to that ensured within the EU (including, where applicable, the implementation of additional safeguards as described in the CJEU's "Schrems II" ruling, and in particular against requests for access to TravelPerk's personal data by law enforcement or public authorities)?
- If the answer to the question above is "Yes", please describe how you ensure that your sub-processors provide such adequate level of protection to personal data, including any onward transfers from your sub-processors to other processors (e.g. regular assessment through questionnaires like this one, audits, etc.).
- Have you conducted transfer impact assessments (TIA) to all your non-EEA processors/sub-processors?
- Are you able to demonstrate compliance with the above questions upon TravelPerk's request?

Technical measures – data encryption

- Access to data (unencrypted): Must the data be subject to unencrypted access by you for the performance of your service to TravelPerk?
- Is client data protected using encryption at rest?
- Is data encrypted during transit?
- Do you enforce using TLS v1.2 or later, with older versions of TLS and SSL prevented via technical means?
- Do you keep the encryption keys yourself or do you appoint an independent third party for such purpose?
- Please describe your encryption key management process (e.g., how do you generate, administer, store or revoke the encryption keys)
- Have you built any back doors (in hardware or software) or similar programming into your services that could be used to circumvent your security measures and to access the systems and/or personal data?
- Have you implemented appropriate technical and organisational measures (see Article 32 GDPR) for every step of the processing operations which ensure that mass and indiscriminate processing of personal data by or on behalf of authorities in transit is made impossible?

- Do you transfer TravelPerk's personal data to your sub-processors using strong encryption before transmission?
- Does the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them?
- Does the strength of the encryption take into account the specific time period during which the confidentiality of the encrypted personal data must be preserved?
- Is the encryption algorithm flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification?
- Are the encryption keys reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked)?

GDPR compliance

- Do you have procedures in place to inform TravelPerk without undue delay in the event of a security incident involving personal data?
- Is data protection training provided to your employees who are processing TravelPerk's personal data?
- Have employees who will have access to TravelPerk's personal data committed themselves to confidentiality or are they under an appropriate statutory obligation of confidentiality?
- Do you have a GDPR-compliant data protection policy for employees?
- Have you got in place a record of processing activities?
- Has a Data Protection Officer (DPO) or data protection responsible been appointed?
- Have you had any contact during the last year with any data protection supervisory authority, either for a complaint, prior consultation, breach notification, etc.?

Data access requests by law enforcement and public authorities

- Have you received any requests from law enforcement or public authorities to disclose your customers' data in the last 5 years?
- Which security measures have you put in place in case law enforcement or public authorities in your country would require disclosure of TravelPerk's personal data?

- Do you have any internal guidelines for dealing with requests from law enforcement and public authorities?
- Before disclosing personal data to law enforcement or public authorities, have you implemented a procedure to check that the request is valid, limited, specific, particularised, and made under enforceable legal process?
- What guarantees do you propose in terms of information prior to granting a request for access from a state service, and in particular an intelligence service, and on your ability to ensure compliance with the principles of necessity and proportionality?
- If legally permitted, will you notify TravelPerk of any request you may receive from law enforcement or public authorities to disclose TravelPerk's data?
- In case you were explicitly prohibited by law from notifying TravelPerk of such requests, will you undertake any actions needed to obtain a waiver of the prohibition, with a view to communicate as much information to TravelPerk and as soon as possible?
- Will you document any actions you undertake (according to the previous question) in order to be able to demonstrate them to TravelPerk upon request?
- Is there any collaboration between you and the public authorities of your country which would allow them access to the personal data held by you and enable them to reconstitute and exploit the content of such personal data?
- Do you publish any transparency report documenting the requests you have received from law enforcement and/or public authorities for access to your customers' data? (e.g. transparency reports describing the type of request, the number of such requests received, and whether content data or non-content data was disclosed)

Specific questions for U.S. vendors

<u>Law Enforcement</u>

- How would you respond to a request by law enforcement (subpoenas, court orders, search warrants and National Security Letters or FISA orders) which implied disclosure of the personal data you process on behalf of TravelPerk?
- How would you respond to a request by any US government or public entity (other than law enforcement) which implied disclosure of the personal data you process on behalf of TravelPerk?
- Have you built any backdoors or other methods into your services to allow any US public authorities to circumvent your security measures and have access to the personal data you process on behalf of TravelPerk?

Direct Application of 50 U.S.C. § 1881a (= FISA 702)

- Do you or any other relevant US entity (controller or processor) that processes or has access to personal data that is transferred to you fall under one of the following definitions in 50 U.S.C. § 1881(b)(4), that could render you or the other entit(ies) directly subject to 50 U.S.C. § 1881a (= FISA 702)?
- [A] Are you or any other relevant US entity a telecommunications carrier, as that term is defined in section 153 of title 47 U.S.C.?
- [B] Are you or any other relevant US entity a provider of electronic communication service, as that term is defined in section 2510 of title 18 U.S.C.?
- [C] Are you or any other relevant US entity a provider of a remote computing service, as that term is defined in section 2711 of title 18 U.S.C.?
- [D] Are you or any other relevant US entity 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?
- Are you or any other relevant US entity an officer, employee, or agent of an entity described in [A], [B], [C], or [D] above?

Processing under EO 12.333

- Do you, or any other relevant US entity (controller or processor) that processes personal data that is transferred from us to you, cooperate in any respect with US authorities conducting surveillance of communications under EO 12.333, should this be mandatory or voluntary?

Other relevant Laws

- Are you or any other relevant US entity (controller or processor) that processes personal data that is transferred from us to you subject to any other law that could be seen as undermining the protection of personal data under the GDPR (Article 44 GDPR)?

- Measures against Mass and Indiscriminate Processing in Transit (FISA 702 and EO 12.333)

- Have you implemented appropriate technical and organisational measures (see Article 32 GDPR) for every step of the processing operations which ensure that mass and indiscriminate processing of personal data by or on behalf of authorities in transit (such as under the “Upstream” program in the US) is made impossible?

* * *