PANDA DOC – DATA TRANSFER IMPACT ASSESSMENT

- **Requirements for Transfers of Personal Data Outside the EEA, Switzerland, and/or the UK.** As a general rule, transfers of personal data which originate in the EEA, Switzerland, and/or the UK to a country that has not been found to provide an "adequate" level of protection (each a "**Third Country**") are only permitted where such transfers are supported by "appropriate safeguards." The most common "appropriate safeguards" used by companies to support the transfer of EEA, Swiss, and/or UK personal data to Third Countries are the EU Standard Contractual Clauses; the UK International Data Transfer Agreement or Addendum; or the EU Standard Contractual Clauses amended as applicable to the Swiss Federal Data Protection Act.

- **Data Transfer Impact Assessments and Related European Data Protection Board ("EDPB") Guidance.**

    - **Data Transfer Impact Assessments:** Following the decision of the Court of Justice of the European Union in the Case C-311/18: Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems ("***Schrems II***"), data exporters and data importers are also required to carry out an assessment of each Third Country's laws and/or practices in force that "may impinge on the effectiveness of the appropriate safeguards of the transfer tools [the data exporter is] relying on, in the context of [the data exporter's] specific transfer" of personal data to the Third Country.[1]

    - **Related EDPB Guidance:** However, under the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 ("**EDPB Recommendations on Supplementary Measures**"), *even if the data transfer impact assessment reveals the Third Country's legislation is "problematic,"*[2] *then the parties may still proceed with the transfer of personal data to the Third Country if the parties are able to demonstrate and document that they have no reason to believe that the Third Country's problematic laws (if any) will be interpreted and/or applied in practice so as to cover the parties' transfer of personal data to the Third Country*.[3]

    - **EU Standard Contractual Clauses:** Clause 14 requires that for all transfers of personal data (regardless of whether they originate from, or are received by, a controller or processor) the parties must warrant that they have "no reason to believe the laws and practices in the third country of destination applicable to the processing of personal data by the

---

[1] European Data Protection Board, *EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0*, June 18, 2021, (hereinafter EDPB Recommendations on Supplementary Measures), at 14, available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[2] "Problematic legislation" is understood as legislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognized by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognized in Union or EU Member States' law, such as those listed in Article 23 (1) GDPR.

[3] EDPB Recommendations on Supplementary Measures at 17 – 18.

data importer . . . prevent the data importer from fulling its obligations under these Clauses."[4] The data importer specifically warrants that it has "made its best efforts to provide the data exporter with the relevant information" to complete the assessment,[5] and the Parties jointly agree to "document the assessment . . . and make it available to the competent supervisory authority on request."[6]

- **Problematic Legislation in the United States – EO 12333 and FISA Section 702.** On the record before it in *Schrems II*, the CJEU considered Executive Order 12333 and FISA Section 702 to be "problematic legislation."

- **Data Transfer Impact Assessment Summary – EO 12333 and FISA Section 702 Likely Do Not Apply**. *The processing that PandaDoc (and its subprocessors) engage in under the agreement is likely not subject to Executive Order 12333 or FISA Section 702. As a result, transfers to PandaDoc and its subprocessors in the United States are likely permitted pursuant to the EDPB Recommendations on Supplementary Measures*.[7]

- **Executive Order 12333 Likely Does Not Apply**. Executive Order 12333 governs how United States' intelligence agencies carry out surveillance *outside the United States* with respect to non-U.S. persons to whom the United States Constitution and laws do not apply. Executive Order 12333 likely has limited to no relevance to transfers of EEA, Swiss, or UK personal data to the United States as *it generally applies to surveillance activities that are conducted wholly outside of the United States*. Accordingly, it's unlikely that Executive Order 12333 would apply to transfers of personal data to PandaDoc or its subprocessors to or within the United States.

- **FISA Section 702 Likely Does Not Apply**. FISA Section 702 (codified at 50 U.S.C. § 1881a) permits the United States government to conduct certain surveillance of non-US persons located outside of the United States through compelled assistance of electronic communication service providers. Surveillance under FISA Section 702 is restricted to specific areas of national defense, national security, and the conduct of foreign affairs, with an emphasis on international terrorism, sabotage, the proliferation of weapons of mass destruction, and other grave hostile acts.

    - **FISA Section 702's Limited Scope – Only Foreign Intelligence Information.** In specific, *FISA Section 702 only permits targeting of individuals where a significant purpose is to obtain "foreign intelligence information."*

      When acquired from a non-U.S. person, "*foreign intelligence information" can generally be thought of as information which relates to the United States' foreign affairs with or national defense against a "foreign power" or "foreign territory"*

[4] EU (New) Standard Contractual Clauses (all Modules) Clause 14(a).
[5] EU (New) Standard Contractual Clauses (all Modules) Clause 14(c)
[6] EU (New) Standard Contractual Clauses (all Modules) Clause 14(d).
[7] EDPB Recommendations on Supplementary Measures at 17 – 18.

or the United States' ability to protect against serious attacks of a "foreign power." The full definition of "foreign intelligence information" can be found in **Exhibit A**.

- **PandaDoc Likely Will Not Process Foreign Intelligence Information.** The transfers of EEA, Swiss, and UK personal data to PandaDoc and its subprocessors in the United States will primarily consist of First and last names, phone number, email, company name, job role, credit card information [insert any other categories of personal data to be transferred]. *This personal data likely will not meet the definition of "foreign intelligence information" under FISA Section 702*.

  A white paper published by the United States Department of Commerce, the United States Department of Justice, and the United States Office of the Director of National Security supports this view and states, "[c]ompanies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data."[8]

  Additionally, PandaDoc provides the following safeguards for personal data stored in the United States:

  1. Personal Data will be transported to the United States and stored in an encrypted fashion.
  2. The keys for decrypting Personal Data concerning individuals in Europe will not be provided to a government authority absent court order unless (1) any impacted individual in Europe has been notified of the government request, or (2) the Data Importer determines that the protection of the rights and freedoms of others requires the disclosure.
  3. Data Importer has, and will maintain, a written policy and procedure for responding to requests from law enforcement agencies (the "Law Enforcement Request Policy").
  4. The Law Enforcement Request Policy requires the Data Importer to determine whether a government request for information is validly issued and authentic.
  5. The Law Enforcement Request Policy requires the Data Importer to inform a government agency that requests Personal Data that such Personal Data includes information about individuals located in Europe.
  6. The Law Enforcement Request Policy requires the Data Importer to attempt to narrow requests for the Personal Data of individuals in Europe to the minimum data needed by the government agency.
  7. The Law Enforcement Request Policy requires the Data Importer to inform a government agency that requests the Personal Data of individuals in Europe that the GDPR, and other European data privacy laws, confer certain

[8] United States Department of Commerce, United States Department of Justice, United States Office of the Director of National Security, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II White Paper*, September, 2020, at 2, available at https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

rights upon individuals located in Europe including, among other things, rights to transparency, access, rectification, and deletion about, and relating to, any entity, including government agencies, that process personal information.

8. The Law Enforcement Request Policy requires the Data Importer to request that the government agency permit the Data Importer to notify the Data Exporter and/or any impacted individuals in Europe of the request prior to any information being transmitted to the law enforcement agency.
9. The Law Enforcement Request Policy requires the Data Importer to request that the government domesticate any request through counterpart agencies located within the European Union.
10. The Law Enforcement Request Policy requires the Data Importer to evaluate whether the request seeks information which goes beyond what appears reasonably necessary for (a) national security, (b) defense, (c) public security, (d) the prevention, investigation, detection and prosecution of criminal offenses, or the breach of ethics for the regulated professions, (e) other important economic or other financial interests of a country, (f) the protection of individuals, or (g) the protection of the rights and freedoms of others.
11. To the extent that the request is determined to be unreasonable, the Law Enforcement Request Policy requires the Data Importer to appeal, narrow, or attempt to quash the request, to the extent permitted by law.
12. The Data Importer will work with the Data Exporter to consider, and evaluate, any additional supplemental measures recommended by the European Data Protection Board ("EDPB").

To date, PandaDoc has never received a government request under either FISA 702 or EO 12333**.**

In light of the above, PandaDoc likely will not process "foreign intelligence information" and therefore PandaDoc's (and its subprocessors') processing of EEA, Swiss, and/or UK personal data under the agreement likely is not subject to FISA Section 702.

- **Conclusion: Transfers of Personal Data to PandaDoc and its Subprocessors in the United States are Likely Permitted.** In light of the information provided in this document, including PandaDoc's practical experience dealing the technical, contractual, and organizational measures PandaDoc has implemented to protect customer personal data, PandaDoc considers that the risks involved in transferring and processing European personal data in/to the US do not impinge on our ability to comply with our obligations under the EU SCCs (as "data importer") or to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.

  PandaDoc has demonstrated and documented that it has no reason to believe that these problematic laws will be interpreted and/or applied in practice so as to cover the transfer of EEA, Swiss, and/or UK personal data to the PandaDoc or its

subprocessors in the United States. As a result, transfers of EEA, Swiss, and/or UK personal data to PandaDoc and its subprocessors in the United States are likely permitted pursuant to the EDPB Recommendations on Supplementary Measures.[9]

[9] EDPB Recommendations on Supplementary Measures at 17 – 18.

Exhibit A – Definition of Foreign Intelligence Information under FISA Section 702

When acquired from a non-U.S. person, "*foreign intelligence information" is defined as*:

(1) *information that relates to … the ability of the United States to protect against* –

(A) *actual or potential attacks* or other grave hostile acts *of a foreign power or an agent of a foreign power*;

(B) sabotage, *international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power*; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power by an agent of a foreign power;

or

(2) *information with respect to a foreign power or foreign territory that relates to* …

(A) *the national defense or the security of the United States*; or

(B) the conduct of the foreign affairs of the United States.