Transferring Personal Information to FIA-Tech – A Statement about the Efficacy of the Standard Contractual Clauses & Essential Guarantees for Surveillance Measures.

Scope & Usage of this Statement

This analysis applies to all FIA Tech products and services. You may only use this statement as part of your internal assessment of the efficacy of using the EU standard contractual clauses as they may apply to your cross-border transfer of personal information. This statement does not constitute legal advice.

Background

FIA Tech deploys many technical and organizational measures to protect personal information from unauthorized processing and to optimize individuals' rights in their data. One such measure is the appropriate use of the standard contractual clauses ("clauses") to safeguard the transmission of personal information to the U.S. The clauses are an effective means to provide GDPR-equivalent protections and rights to data subjects given the technological and organizational measures FIA Tech undertakes to reduce certain risks, including the differences between US and EU laws.

Prior to reaching this conclusion, FIA Tech performed the analysis dictated in the European Court of Justice's ("EUCJ") Schrems-II decision and assessed the concerns identified by the European Data Protection Board's ("EDPB") "Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures." We also took into consideration the scenarios outlined in the EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data."

Understanding the Nature and Amount of Personal Information Transferred.

The first step in the Schrems-II analysis is to understand the personal information to be transferred.

Your account administrator will upload standard B2B contact information regarding individual employees assigned to perform specific roles on your organization's behalf. This profile information will include the employee's name, email, telephone number, position, and information about the person's authority to execute contracts ("User Profiles"). User Profile information is, generally, public -- of the kind found on a corporate website or a LinkedIn profile.

The number of User Profile records likely to be transmitted depends on the size of your organization. Typically, system users only permit a limited number of individuals to create profiles. As a result, the amount of personal information transferred to FIA Tech is often exceedingly small. Although User Profiles contain GDPR-protected personal information there is relatively low risk in transmitting this type of information. The personal information used in FIA Tech systems is not sensitive or special, is easily obtained through public information, and is of exceedingly low volume.

For users of the OCR service, OCR is a service used to report account information directly to the US government. This is a requirement of US law to aid in combatting fraud and providing other security in public markets. Transmitted information is also shared with some exchanges. Transmissions to exchanges occur after the importation into the United States. Cross-border transmissions for the purpose of OCR is a permitted derogation under GDPR Article 49.1(d) as the transmission is in the public interest and to uphold law. (See, generally, discussion of public interest derogations in ICO letter to the U.S. Securities and Exchange Commission, Sept 11, 2020 https://ico.org.uk/media/2619110/sec-letter-

20200911.pdf) (“SEC Advisory Letter”) Reporting for OCR purposes is substantially the same as the types of transmissions assessed in the SEC Advisory Letter.

Assessing US law and whether it will impinge on the clauses effectiveness.

The next step is to assess if there is anything in the US law that may impinge on the clauses' effectiveness when coupled with the technical and organizational measures adopted by FIA Tech. Concerning transfers to the US, the EUCJ focuses on whether transmissions are subject to direct surveillance under either: (1) Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") or (2) vulnerable to mass surveillance measures authorized under Executive Order 12 333 ("EO 12 333").

Neither of these sections apply to FIA Tech.

Transmissions to FIA Tech are not vulnerable to direct surveillance under FISA Section 702 because FIA Tech is outside of the scope of Section 702. FIA Tech does not fall within the definitions of a "provider of electronic communications” or the definition of a provider of "remote storage."

Transmissions to FIA Tech are not likely to fall under the second prong of the EUCJ’s concerns, namely, mass surveillance. FIA Tech offers technological measures that are believed to protect transmissions from mass surveillance, under EO 12 333. FIA Tech offers encryption in transit using TLS 1.2 and 1.3. These protocols were primarily developed in response to the Snowden revelation that TLS 1.1. and other protocols were susceptible to penetration by US authorities prior to arriving for storage within the US.

Today, if your organization appropriately configures communications using TLS 1.2 or 1.3, the transfer of a User’s Profile is unlikely to be penetrated in transit by the US government. Indeed, this level of encryption is the method advocated by Mr. Snowden currently to avoid surveillance by governments.

Conclusion

There is no reason to believe FIA Tech will be prevented (by US laws or government surveillance) from fulfilling its obligations under the Clauses or that it would fail to provide protections to EU or UK data subjects that are equivalent to that provided in those jurisdictions.