BarentsKrans

6 November 2023

EU-US Data Privacy Framework for SkyKick

Review of Implementation and Measures

dedicated

Data Privacy Framework

How does the Data Privacy Framework work?

- On 10 July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to US companies participating in the EU-U.S. Data Privacy Framework.

- With the EU-U.S. Data Privacy Framework, European entities can transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

- U.S. companies can certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with EU-U.S. Data Privacy Framework Principles. The U.S. Department of Commerce is responsible for the certification and monitoring of these companies. Compliance will be enforced by the US Federal Trade Commission.

- SkyKick has certified its compliance to the EU-U.S. Data Privacy Framework and the EU-U.S. Data Privacy Framework Principles.

Data Privacy Framework

Additional safeguards necessary?

- The adequacy decision follows the US' signature of an Executive Order on ‘Enhancing Safeguards for United States Signals Intelligence Activities', which introduced new binding safeguards.
- For instance, US public authorities’ access to data is limited to what is necessary and proportionate to protect national security. Also, EU individuals will have access to an independent and impartial redress mechanism.
- The safeguards established by the US Government are applicable to all data transfers under the GDPR to US-based companies, irrespective of the transfer mechanisms used. The safeguards therefore also facilitate the use of other tools, such as the European Commission’s Standard Contractual Clauses (SCCs).
- Since the safeguards put in place by the US will also apply when data is transferred by using other tools (including SCCs), supplementary measures are not necessary.
- SkyKick relies on the SCCs for the transfer of personal data from the EU to the US. Considering the above, this suffices as appropriate safeguard for transfers to the US, without the need for supplementary measures.
- Despite it not being necessary, SkyKick has taken various supplementary measures to increase personal data protection and security. The following slides provide an overview of such measures, including where evidence of implementation can be found. This overview, which is based on information provided by SkyKick and public sources, has been last updated on 6 November 2023.

Data Privacy Framework

Organizational Measures – 1 of 2

- The following organizational strategies have been implemented by SkyKick to help achieve an essentially equivalent level of data protection:
  1) For its End-Customers located in the European Economic Area, United Kingdom or Switzerland, SkyKick has structured its products such that they are not subject to the jurisdiction of the United States.
  2) SkyKick provides the service through a foreign affiliate (SkyKick B.V., located in the Netherlands) that is not subject to the jurisdiction of US law.
  3) SkyKick has appointed a Data Protection Officer who is registered with the Dutch Supervisory Authority (Autoriteit Persoonsgegevens) and who serves as the main point of contact for any inquiry related to privacy for the organization, its customers and the authorities.

This strategy addresses issues with all relevant US surveillance laws for all SkyKick's products.

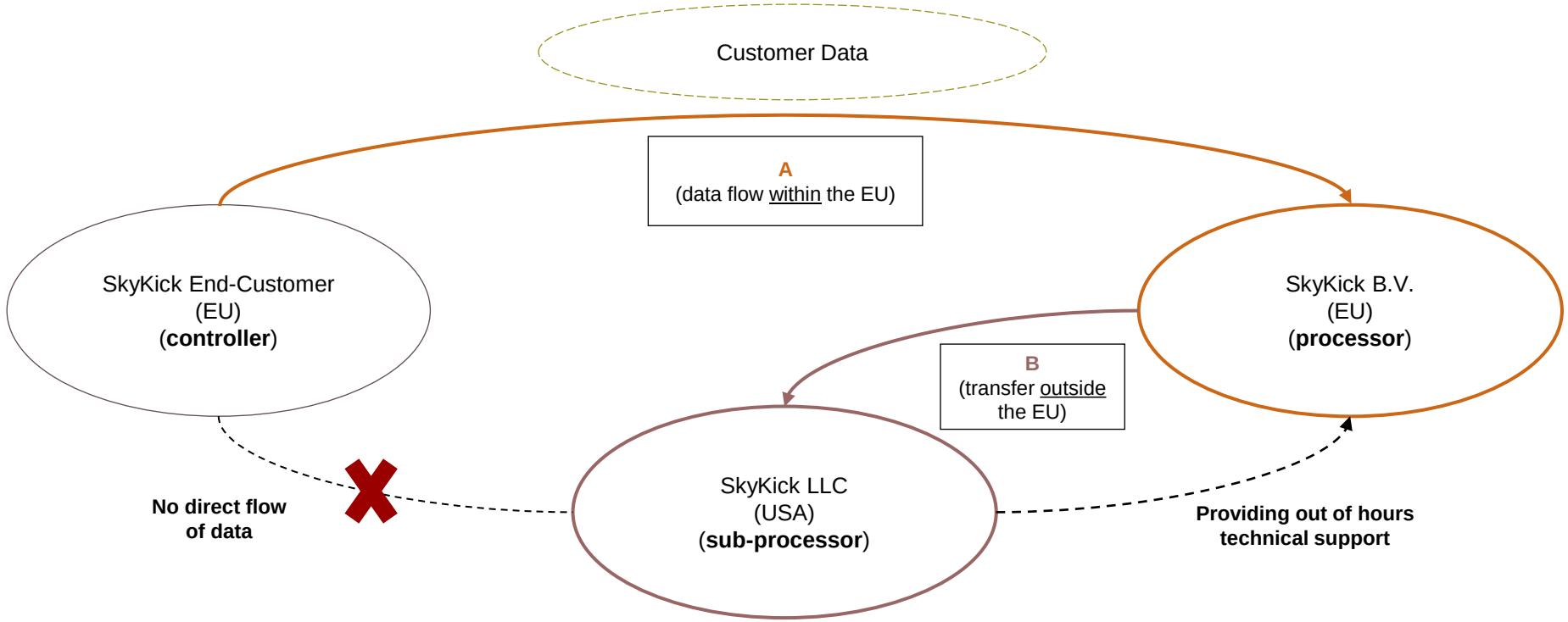
SkyKick implemented this strategy internally via contractual agreements between SkyKick LLC and SkyKick B.V. and included a provision in its Customer Terms & Conditions.

The next slide contains a visual representation of the contracting structure.

Data Privacy Framework

Organizational Measures – 1 of 2

Contractual structure



Data Privacy Framework

Organizational Measures – 2 of 2

SkyKick will document and record any government access request and the response provided, including the legal reasoning and SkyKick End-Customer/data subject involved, and will make the records available to SkyKick End-Customers upon request.

(*EDPB 01/2020 Recommendations to Supplement Transfer Tools, page 44*)

- SkyKick is upholding the EU transparency principle by providing clear, relevant information for each government request it receives.
- This strategy addresses issues with all relevant US surveillance laws for all SkyKick's products.
- SkyKick implemented this strategy internally by developing a suitable company policy and by inserting a commitment in the publicly posted Customer Terms & Conditions.

Data Privacy Framework

Supplemental Technical Measures – 1 of 2

SkyKick conducts security and privacy audits, using external providers, and will conduct such audits on a regular basis, to ensure that:

a) there are no back doors or similar vulnerabilities in its products that could be used by government agencies to access personal data; and

b) none of its business processes unintentionally facilitate government access to data its product retain.

(*See EDPB 01/2020 Recommendations to Supplement Transfer Tools, page 38*)

This strategy addresses issues with all relevant US surveillance laws for all SkyKick's products.

SkyKick implemented this strategy internally by retaining a suitable auditor to perform regular security & privacy audits. SkyKick will regularly revise its security measures to ensure that SkyKick is up-to-date regarding the latest innovations and trends in data protection.

Data Privacy Framework

Supplemental Technical Measures – 2 of 2

SkyKick has implemented a modified “Warrant Canary” mechanism so that the public, regulators and SkyKick End-Customers can visit a web portal to confirm that, to date, SkyKick has not received any confidential requests for access to SkyKick End-Customer information (the mechanism does not include requests for which SkyKick is permitted by law to notify the relevant SkyKick End-Customer).

(*See EDPB 01/2020 Recommendations to Supplement Transfer Tools, page 38*)

If SkyKick were to receive a confidential access request, the mechanism will disclose that SkyKick has received a request and identify steps that: (a) SkyKick is taking to challenge the request; and/or (b) SkyKick End-Customers can take to support SkyKick’s opposition or protect their own interests.

This strategy addresses issues with all of the relevant US surveillance laws for all of SkyKick’s products.

SkyKick is highly unlikely to ever receive a confidential request, so this measure should provide assurances to regulators and customers.

Data Privacy Framework

Contractual Measures – 1 of 2

SkyKick has committed to challenge all FISA warrants on behalf of the affected individual before the independent Data Protection Review Court (DPCR) on the basis that the warrant does not meet FISA requirements or is otherwise unlawful.

(*See Adequacy decision for the EU-US Data Privacy Framework, page 52)*

- SkyKick will seek to argue, among other things, that access to SkyKick's data by the US government is unlawful and adversely affects the privacy and civil liberties interests of the affected individual.
- This strategy addresses issues with FISA for all SkyKick's products.
- SkyKick implemented this strategy by inserting sufficient commitments in its Customer Terms & Conditions stating that it will challenge, to the maximum extent possible, any access requests it receives.

Data Privacy Framework

Contractual Measures – 2 of 2

SkyKick has committed to challenge (i.e., quash, modify, or limit) all Stored Communications Act (SCA) and SCA-like state law warrants, subpoenas, and court orders on the basis of all potential legal grounds.

(*See EDPB 01/2020 Recommendations to Supplement Transfer Tools, page 40*)

This strategy addresses issues with SCA and SCA-like state laws for all SkyKick's products.

SkyKick implemented this strategy by inserting a sufficient commitment in its Customer Terms & Conditions stating that it will challenge, to the maximum extent possible, any access requests it receives.

Data Privacy Framework

Supplemental measures overview

Supplemental measure	In place?	Link
SkyKick provides the service through a foreign affiliate, SkyKick B.V., located in the Netherlands, that is not subject to the jurisdiction of US law.	✓	SkyKick Customer Terms & Conditions, Article 5.3
SkyKick will document and record any government access request and the response provided and will make the records available to SkyKick End-Customers upon request.	✓	Any request, and response provided, is maintained in the records of the Data Protection Officer. The Data Protection Officer can be reached via dataprivacy@skykick.com
SkyKick will conduct a security & privacy audit using an external provider.	✓	SkyKick Data Processing Addendum, Article 5 SkyKick ISO 27001:2013 Certificate & Statement of Applicability V4.0 SkyKick ISO 27701:2019 Certificate & Statement of Applicability V5.0 SkyKick Data Pro Certificate
SkyKick has implemented a modified “Warrant Canary” mechanism.	✓	SkyKick confirmed to us that its Trust Center and the blog functionality therein serve as this mechanism.
SkyKick has committed to challenge all FISA warrants, on behalf of the applicable data subject.	✓	SkyKick Customer Terms & Conditions, Article 3.3
SkyKick has committed to challenge (i.e., quash, modify, or limit) all SCA and SCA-like state law warrants, subpoenas, and court orders.	✓	SkyKick Customer Terms & Conditions, Article 3.3