AvePoint Transfer Impact Assessment (TIA) Frequently Asked Questions

Updated on January 13, 2023

The Schrems II judgment of the European Court of Justice (ECJ), invalidating the Privacy Shield as an international transfer mechanism, has raised questions among our global customers. While the European Commission and the US Department of Commerce work to find a reliable and legally compliant solution, we at AvePoint have been taking appropriate steps to ensure an adequate level of protection of our data transfers.

This document summarizes the main findings of the Transfer Impact Assessment (TIA) conducted by AvePoint, which our customers may use to gather relevant information for their independent assessment of vendors and partners.

What Is Schrems II

Schrems II is the commonly used name for the ECJ case C-311/18. On 16 July 2020, the ECJ decided that the EU-US Privacy Shield would be invalid and could no longer be used as a personal data transfer mechanism to safeguard the transfer of personal data to the US. Data exporters (companies transferring personal data outside of the European Union (EU)/European Economic Area (EEA)), where appropriate with the collaboration of the data importer (the company in a third country receiving the personal data from the data exporter directly or indirectly), will now have the responsibility to verify, on a case-by-case basis, if the law and practices of the non-EU third country provide "essentially equivalent" protection for personal data transferred from the EU/EEA. When conducting this analysis, the parties must consider, among other things, the circumstances of transfer, nature of the data, and the availability of possible additional safeguards (i.e., supplementary measures).

What Is a Transfer Impact Assessment (TIA) And Why Is It Relevant?

A Transfer Impact Assessment – or TIA – is a documented assessment of a transfer of personal data from the EU/EEA to non-EU/EEA countries that do not benefit from an adequacy decision of the European Commission (here's the list of countries benefiting from an adequacy decision). TIAs are required to be conducted under the new Standard Contractual Clauses and serve to document a proper assessment of risks associated with the transfer. This is particularly relevant for transfers to the US, as the Privacy Shield has been invalidated by the ECJ in its "Schrems II" decision. Because AvePoint provides its services globally, AvePoint is committed to ensuring that if and when personal data is transferred to a non-EEA country on our watch, the relevant legal obligations are met.

What Are the Standard Contractual Clauses (SCCs)?

SCCs are standard contractual terms that have been pre-approved by the European Commission and serve as one of the legal transfer mechanisms to allow personal data to flow

outside of the EU/EEA. The EU Commission published an updated version of the SCCs on 4th June 2021 to modernize the SCCs, account for sub-processors and additional models (e.g., Processor to Controller, and Processor to Processor) and add additional contractual safeguards in response to the Schrems II decision.

All affiliated companies of AvePoint (including the US-based companies) have reciprocally submitted to the EU Commission's SCC, meaning that the legally required adequate level of protection for a transfer of personal data to a third country can still be demonstrated without relying on Privacy Shield. AvePoint has also conducted Transfer Impact Assessments for its operations in third countries where no adequacy decision by the EU Commission exists.

How Are AvePoint Services Relevant Under This Decision?

AvePoint provides its services on a global scale and as an international organization and has offices in various countries. As such, even though customers may retain their own tenant data in a regional data center of their choice, customer information may be accessed by our employees around the world on a need-to-know basis, for example in order to be able to support our customers in various parts of the services (sales, billing and payment, technical support and maintenance, fraud detection and prevention, etc.). You can find more detailed information on how AvePoint protects and secures data in our Data Protection and Information Security Policy | AvePoint

Can Transfers of Personal Data to The US Continue?

Yes. In the same Schrems II ruling, the ECJ confirmed that the Standard Contractual Clauses remain a valid transfer mechanism, subject to certain conditions. The European Data Protection Board (EDPB) states in its guidance, that transfer mechanisms such as SCCs, may need to be paired with supplementary technical, organizational, and contractual measures as may be appropriate in a particular personal data processing context to provide an adequate level of protection essentially equivalent to the EU standards.

AvePoint relies on SCCs for intracompany transfers of personal data to the US and globally.

We have to date no reason to believe that the laws and practices in the US and the global countries applicable to the processing of personal data in the context of our services prevent AvePoint from fulfilling its obligations under the SCCs. Nonetheless, please note that we do not provide customers with legal advice with respect to their use of the services, for which Customers shall perform their own legal assessment.

What Are Foreign Intelligence Surveillance Act (FISA) 702 And Executive Order (EO) 12333 That Were Mentioned in Schrems II?

FISA 702 and EO 12333 were identified by the ECJ in Schrems II as being potential obstacles to ensuring essentially equivalent protection for personal data in the US:

- FISA Section 702 (“FISA 702”) – allows US government authorities to compel disclosure of information about non-US persons located outside the US for the purposes of foreign intelligence information gathering. This information gathering must

be approved by the Foreign Intelligence Surveillance Court in Washington, DC. In-scope providers subject FISA 702 are electronic communication service providers ("ECSP") within the meaning of 50 U.S.C § 1881(b)(4), which can include remote computing service providers ("RCSP"), as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711.

- Executive Order 12333 ("EO 12333") – authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies to collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire, and other electromagnetic means. This may include accessing underwater cables carrying internet data in transit to the US. EO 12333 does not rely on the compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure.

Further information about these and other US Surveillance Laws may be found in the U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II whitepaper (published by the US Department of Commerce, Department of Justice, and Office of the Director of National Intelligence), which discusses the limits and safeguards relevant to US public authority access to data in response to Schrems II.

Is AvePoint Subject to US Surveillance Laws (Such As 50 USC § 1881 (B) (4), And Thus Directly Subject To 50 USC § 1881a (= FISA 702)?)

AvePoint has not received any orders or other guidance from the relevant authorities indicating that it is directly subject to FISA 702. Generally, the definition of electronic communication service provider under 50 USC § 1881 (b) (4) includes telecommunications carriers (e.g., AT&T, T-Mobile, Verizon), providers of electronic communications services and remote computing services (e.g., Facebook, Google, and AWS), as well as any other communications service providers that have access to wire or electronic communications (either in transit or in storage). However, according to guidance issued by the Department of Justice (available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf), the definition could potentially capture any company that provides its employees with corporate email or a similar ability to send and receive electronic communications, regardless of the company's primary business or function.

How Many Disclosure Requests Under FISA 702 Has AvePoint Received?

AvePoint has neither received nor been notified of a National Security Letter, an order under the Foreign Intelligence Surveillance Act, or any other classified request for user information pursuant to the national security laws of the United States or any other country.

Does AvePoint Provide a Periodic Transparency Report Detailing Criminal Process or National Security Disclosure Requests?

Due to its current minimal, if any, exposure to disclosure requests, AvePoint has decided not to publish periodic transparency reports at this point in time. AvePoint will monitor any developments in this regard and may revise its policy accordingly.

What Is the Purpose of The Transfer?

To provide our customers with flexible and reliable solutions, AvePoint may transfer personal data in order to be able to support our customers in various parts of the services (sales, billing and payment, technical support and maintenance, fraud detection and prevention, etc.). You can find more detailed information on the purposes of the transfers in our Data Protection and Information Security Policy | AvePoint

Who Is the Data Importer(s) Under the SCCs?

Data Importer(s):

Identity:	The data importer is the party as identified in the relevant agreement between AvePoint and the customer.
Contact Person's Name:	The data importer's contact is specified in the relevant agreement between AvePoint and the customer.
Activities Relevant to Data Transferred Under These Clauses:	The relevant activities are specified in the relevant agreement between AvePoint and the customer.
Role:	The data importer is the processor.

What Data Is Affected?

You can find a complete list of categories of data affected in our Data Protection and Information Security Policy | AvePoint for information on the nature of AvePoint's processing activities in connection with the provision of the Services, the types of customer personal data we process, and transfer, and the categories of data subjects. Customer information may be accessed by our employees from our offices locations around the world) in order to provide the services and support our customers.

What Sub-Processors Does AvePoint Use?

List of AvePoint Sub-Processors:

Schedule 4 – Sub-processors

This table lists the initial sub-processors of AvePoint as Annex III to the SCC (or processors, in the case of a controller-to-controller relationship). The contact persons' names, positions and contact details are specified in the Agreement.

Name	Address	Description of Processing[1]			
		Cloud Ops	Support	SMEs	Internal
AvePoint, Inc. (including various offices within the United States)	525 Washington Boulevard, Suite 1400, Jersey City, NJ 07310, USA	Yes	Yes	Yes	Yes
AvePoint Public Sector, Inc.	2111 Wilson Boulevard, Suite 920 Arlington, VA 22201, USA	No	Yes	Yes	Yes
AvePoint Holdings USA, LLC	901 East Byrd Street, Ste. 900, Richmond, VA 23219, USA	No	Yes	Yes	Yes
	Branch office at: Suite B, 6th Floor, Net One Center, 26th st. cor. 3rd Avenue, E-Square Zone, Crescent Park West, Bonifacio Global City, Taguig, 1634, Metro Manila, Philippines	No	Yes	Yes	Yes
AvePoint AU Pty Ltd	Level 11, 459 Collins Street Melbourne, VIC 3000 Australia	No	Yes	Yes	Yes
	Sydney, Australia Square Plaza Level 12, 95 Pitt Street Sydney, NSW 2000, Australia	No	Yes	Yes	Yes
AvePoint Canada, Ltd.	Suite 1700, Park Place, 666 Burrard Street, Vancouver, BC V6C 2X8, Canada	No	Yes	Yes	Yes
AvePoint UK, Ltd.	Watchmaker Court, 33 St John's Lane, London EC1M 4BJ, United Kingdom	No	Yes	Yes	Yes
	Branch office at: AvePoint South Africa Block A Wedgefield Office Park, 17 Muswell Road South, Johannesburg, Gauteng, 2021, South Africa	No	Yes	Yes	Yes
AvePoint Deutschland GmbH	Nymphenburger Str. 3, 80335 Munich, Germany	No	Yes	Yes	Yes
	Branch offices at: AvePoint Benelux, New Babylon Gardens Anna van Buerenplein 41, 2595 DA Den Haag, The Netherlands	No	Yes	Yes	Yes
	AvePoint France, 24-32 Boulevard Gallieni 92130 Issy-les-Moulineaux, France	No	Yes	Yes	Yes
	AvePoint Sweden, Malmskillnadsgatan 32, 111 51 Stockholm, Sweden	No	Yes	Yes	Yes
	AvePoint Schweiz (Switzerland), Bahnhofstrasse 52, 8001 Zürich, Switzerland	No	Yes	Yes	Yes
AvePoint Japan K.K.	Keikyu Daiichi Building 11th Floor, 410-18 Takanawa Minato-ku, Tokyo 108-0074, Japan	No	Yes	Yes	Yes
AvePoint Singapore Pte. Ltd.	10 Collyer Quay, Level 17, Unit #01/04 Ocean Financial Centre, Singapore 049315	No	Yes	Yes	Yes
MaivenPoint Pte. Ltd.	10 Collyer Quay, Level 17, Unit #01/04 Ocean Financial Centre, Singapore 049315	No	Yes	Yes	Yes
AvePoint Technology Changchun Co. Ltd.	Tellhow Shenlan International Block 4, 10th Floor, Jingyue HiTech Industry Development Zone, No.1550 Tianpu Rd, Changchun 130000, Jilin Province, China	Yes	Yes	Yes	Yes
Shanghai AvePoint Software Technology Corporation Limited	Suite 1105, 21st Century Building 11th Floor, No.210 Century Avenue, Shanghai 200120, China	No	Yes	Yes	Yes
AvePoint Beijing Technology Ltd.	Puxiang Center, Block B, 18th Floor Hongtai East Street, Chaoyang District, Beijing 100102 China	No	Yes	Yes	Yes
AvePoint Vietnam Company Limited	Five Star Tower, No 28bis Mac Dinh Chi Street, Da Kao Ward, District 1, Ho Chi Minh City, Vietnam	No	Yes	Yes	Yes
AvePoint Ontario Ltd.	199 Bay Street, Commerce Court West, 5300, Toronto, Ontario, Canada, M5L 1B9	No	Yes	Yes	Yes
AvePoint Korea Co., Ltd.	Gangnam Financial Plaza 15th Floor #1513, Teheran-ro 419, Gangnam-gu, Seoul, South Korea 06192	No	Yes	Yes	Yes
Combined Knowledge Limited	Watchmaker Court, 33 St John's Lane, London EC1M 4BJ, United Kingdom	No	Yes	Yes	Yes
I-Access Solutions Pte. Ltd.	1003 Bukit Merah Central, Singapore 159836	No	Yes	Yes	Yes

[1] The stated types of Processing have the following meaning:

Cloud Ops: AvePoint's Cloud Operations team operates and maintains the AvePoint Online Services (AOS). The Cloud Operations team is distributed over several countries to ensure proper monitoring of AOS availability around the clock.

Support: AvePoint provides 24/7 product support under a follow-the-sun model. AvePoint offices in the different time zones take over support responsibility during their respective office hours.

SMEs: AvePoint is set up as a modern matrix organization: Subject matter experts (SMEs) are employed by a specific affiliate but may provide services for the whole AvePoint group. An AvePoint SME from, e.g., the UK might be best suited to respond to a customer-specific question or request, even if the contractual relationship between the customer and AvePoint is not in the UK.

Internal: AvePoint Processes Personal Data for a variety of internal reasons (e.g., to maintain the customer relationship) as laid out in AvePoint's Data Protection and Information Security (DPIS) Policy at https://www.avepoint.com/agreements/dataprotection and AvePoint's Privacy Policy at https://www.avepoint.com/company/privacy-policy.

Further, AvePoint Companies use the services of Microsoft Corporation at One Microsoft Way, Redmond, Washington, 98052-6399, USA (including its affiliates). Microsoft operates the Azure infrastructure leveraged by AvePoint for the provision of the AvePoint Online Services and the M365 and O365 environments that are used by AvePoint for various purposes (e.g., usage of the CRM system Dynamics).

Has AvePoint taken any legal, technical, or organizational security measures to ensure that the level of protection is maintained when transferring data to processing in third countries?

Contractual:

All affiliated companies of AvePoint (including the US-based companies) have reciprocally submitted to the EU Commission's standard contractual clause (SCC), meaning that the legally required adequate level of protection for a transfer of personal data to a third country can still be demonstrated without relying on Privacy Shield, which had been invalidated in the Schrems II judgment.

Technical:

From the technical perspective, data handled by AvePoint's cloud and SaaS solutions (AvePoint Online Services or AOS) resides at all times in the customer's Azure tenant and the only data that is stored on the Azure tenant provisioned by AvePoint for the customer in the customer-selected data center is configuration data in an encrypted database, and, depending on the specific AvePoint solution, certain other data generated by the AvePoint solution (e.g. backup files created by AvePoint Cloud Backup). However, all that data will be securely fetched via HTTPS from the respective API and will be AES 256 encrypted immediately afterwards by using either a random key or – if desired and provided that the customer has an Azure Key Vault

subscription – a key provided by the customer. After that, the encrypted data is sent to the selected Azure data center (or, in cases of Bring-Your-Own-Storage, BYOS – to the extent possible for the specific AvePoint solution – to the customer-provided storage) and is stored there. The data can only be used by the customer's AOS instance using the predefined password and AvePoint employees have at no time during that process any access to unencrypted data.

Organizational:

As an organizational matter, AvePoint has achieved and maintains an ISO 27001:2013 certification with respect to secure software development and maintenance process including support business functions like Infosec, Information Technology (IT), Human Resources (HR), Sales and Marketing, Project Management, Operations and Call Center; as well as the System and Organization Controls (SOC) 2 Type II certification for its core business functions. More information about this is available at https://www.avepoint.com/company/privacy-and-security.

More information about this is available at https://www.avepoint.com/company/privacy-and-security.

In addition, any requests for data access by authorities, including law enforcement or intelligence agencies, are subjected to a legal assessment by qualified personnel. AvePoint will inform customers whose data is affected by such requests without undue delay. Access to or disclosure of customer data will only be granted if the legal assessment has determined that there is an applicable and legally valid basis and that the request must be granted on that basis. Any access or disclosure will be limited to the mandatory minimum. Further, AvePoint will seek legal remedy against the request by any means that have an acceptable prospect of success; including, where applicable, lawsuits or measures of injunctive relief. AvePoint will also reasonably cooperate in the customer's own legal defense against the access request.

What Is the Risk?

In light of the information reviewed in our assessment, including AvePoint's practical experience dealing with government requests and the technical, contractual, and organizational measures AvePoint has implemented to protect customer personal data, AvePoint considers that the risks involved in transferring and processing of personal data globally do not impinge on our ability to comply with our obligations under the SCCs (as "data importer") or to ensure that data subjects' rights remain protected.

Why Does AvePoint Still Refer to The Privacy Shield in Its Privacy Notice?

As laid out above, all affiliated companies of AvePoint (including the US-based companies) have reciprocally submitted to the EU Commission's Standard Contractual Clauses (SCC), meaning that the legally required adequate level of protection for a transfer of personal data to a third country can still be demonstrated without relying on Privacy Shield.

Additionally, AvePoint maintains its Privacy Shield certification, as the US Department of Commerce encouraged participants after the Schrems II decision to maintain their adherence to the principles and requirements of the Privacy Shield Framework. The US Department of Commerce continues to administer and enforce the Privacy Shield program. This means that AvePoint still adheres to the Privacy Shield principles in addition to applicable Chapter V

GDPR measures; but does not rely on Privacy Shield for the legality of third country personal data transfers or processing. As an appropriate safeguard in terms of Art. 46 GDPR, AvePoint uses the Standard Contractual Clauses as issued by the EU Commission.