Archer Transfer Impact Assessment

Contents

Summary and Purpose

This Transfer Impact Assessment is conducted pursuant to the requirements set forth in the General Data Protection Regulation 2016/679 on the protection of natural persons in the Processing of Personal Data and on the free movement of such data ("GDPR"), in conjunction with the requirements and principles established in Schrems II[1], the EU SCCs[2], and the European Data Protection Board Recommendations on Supplementary Measures[3] ("EDPB Recommendations"). Under Chapter V of the GDPR, personal data cannot be transferred outside the European Union unless the importing country has been deemed adequate by the European Commission, or the transfer is subject to appropriate safeguards, such as the EU SCCs as described herein.

The requirement to conduct a Transfer Impact Assessment arose as a result of Schrems II, and while Schrems II related to data transfers from the European Union to the United States, the outcome of the requirements laid down by the CJEU was a fundamental change to how organizations can use the EU SCCs, for transfers to all third countries without an adequacy decision, as an appropriate transfer mechanism pursuant to Article 46 of the GDPR.

The obligation arising is for data exporters, with the assistance of data importers, where applicable, to conduct a transfer impact assessment by assessing the local laws and practices of the third country to which data is being exported, to ensure compliance with an essentially equivalent level of protection required under EU law. Provided that the transfer to the entity in the third country provides an essentially equivalent level of protection, then the transfer can be adequately safeguarded using the EU SCCs. If the local laws and practices of the third country potentially result in an inability of the data importer or exporter from fulfilling its obligations under the EU SCCs, then the data importer, in conjunction with the data exporter, must implement appropriate supplementary measures which address the concern giving rise to potential inability in fulfilling its obligations under the EU SCCs.

The Purpose of this Archer Transfer Impact Assessment (hereinafter "TIA") is to assist Archer's customers in conducting their Transfer Impact Assessments. If you require further information relating to Archer's Transfer Impact Assessment, please reach out to privacy@archerirm.com.

1 Judgment of 16 July 2020, case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems

2 The clauses as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and located at https://ec.europa.eu/info/law/law- topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

3 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Scope:

The scope of this TIA applies to data transfers made pursuant to Archer's customers' use of the Archer SaaS Cloud Service Offering.

In connection with your use of the Archer SaaS Service Offering, you, the customer, acts as data exporter, and therefore in accordance with Schrems II, the EDPB Recommendations, and Clause 14 of the EU SCCs, the obligation is on the data exporter to ensure that the relevant transfer remains in compliance with the GDPR.

Archer does, however, have an obligation to provide reasonable assistance to the data exporter in conducting its Transfer Impact Assessment, and also has an obligation to *warrant that they (Archer) have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses.*

This Transfer Impact Assessment is published in order to ensure customer is provided with sufficient information to conduct its Transfer Impact Assessment.

Step 1 Know Your Transfers

Know Your Transfer: The context within which data transfers can occur during use of Archer's Service Offering is customers who are deployed in a data centre environment, other than in the EU, and when customers upload data directly into those environments from within the EU. For example, if a United States customer purchases Archer SaaS and is deployed in the United States data centre environment, then submission of data by a customer authorized user into the SaaS environment, from within the European Union, by that customer authorized user, could be considered a transfer of data by customer, subject to the GDPR international transfers requirements.

Please review the Archer Subprocessors page for further details on locations of processing: https://www.archerirm.community/t5/saas-compliance-security/archer-subproccessors/ta-p/672108

The data transfer consideration, in the context of using the Service Offering, does not typically arise for EU customer's because all EU customers are deployed in the EU data centre, unless they specifically designate otherwise (currently Ireland and Germany) and therefore uploading of Personal Data to the environment, is not a transfer outside the EU.

There are ancillary transfers that could possibly take place for a customer deployed in the EU environment, and this would be in the context of Customer Support, where Personal Data is transferred, and in the context of limited circumstances where Archer would need to access the customer environment, from a third country, in reaction to a security incident (such access only on customer prior approval). Archer's Transfer Impact Assessment for those Customer support scenarios, can be found here.

Onward Transfer

Archer uses Amazon Web Services data centre for providing the environment within which customer data (including personal data) is hosted. Customer's may consider a transfer to be from Customer, as the data exporter, to Archer as the data importer, and then the onward transfer is from Archer to AWS, or Customer's may consider that the transfer is directly from Customer, as data exporter, to AWS as Data Importer. In either case, this Transfer Impact Assessment applies, and the applicable SCCs are incorporated into the contractual arrangement both between Archer and its customers, and Archer and AWS.

Step 2: Identify the transfer tools you are relying on

Archer ensures that the mechanism which is in place to ensure adequate safeguards for the international transfer of Personal Data, in accordance with Article 46 of the GDPR, are the EU SCCs.

For data transfers from the United Kingdom, Archer relies on the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018, and this Transfer Impact Assessment applies as the Transfer Risk Assessment required from a UK data protection laws perspective.

Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer.

Transfers to the United States		
Question	**Answer**	**Notes**
Are there any laws in the US that enable government authorities to access personal data in a manner which would impinge on the effectiveness of the provisions of the SCCs??	Archer is aware of a number of US laws that could, in theory, allow US government authorities to access personal data; however, in practice would not result in an inability of Archer to meet its obligations under the SCCs, and in any event under this regime, following the signing of the Executive Order on "Enhancing Safeguards for United States Signals Intelligence Activities", the Data Privacy Framework was approved, resulting in the designation of the United States as a destination with essentially equivalent safeguards. •Section 702 FISA – contains provisions which can, in some circumstances, allow US government authorities to compel disclosure of information for the purposes of foreign intelligence information gathering. The following is the scope of entities that could be subject to FISA702: - 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 ("EO12333") - authorises intelligence agencies to conduct surveillance outside of the US, potentially	Further information about these US surveillance laws can 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 from September 2020. This whitepaper details the limits and safeguards pertaining to US public authority access to data and was issued in response to the Schrems II ruling. Regarding FISA 702 the whitepaper notes: For most companies, the concerns about national security access to company data highlighted by Schrems II are "unlikely to arise because the data they handle is of no interest to the U.S. intelligence community." Companies handling "ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data." There is individual redress, including for EU citizens, for violations of FISA section 702 through measures not addressed by the court in the Schrems II ruling, including FISA provisions allowing private actions for compensatory and punitive damages. Regarding Executive Order 12333 the whitepaper notes: EO 12333 does not on its own "authorize the U.S.

	providing authority for US intelligence agencies to collect 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.	government to require any company or person to disclose data." Instead, EO 12333 must rely on a statute, such as FISA 702 to collect data. Bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333.
Is Archer subject to Section 702 FISA or EO 12333?	Archer's position in relation to FISA 702 and EO 12333 is that it is unlikely that Archer is directly subject to either legislative provision. In the unlikely event that Archer was deemed to technically be subject to FISA 702 where it is deemed to be a RCSP, Archer does not process personal data that is likely to be of interest to US intelligence agencies, and Archer has never received such requests. Furthermore, in such cases Archer is not likely to be subject to upstream surveillance orders under FISA 702, the type of order principally addressed in, and deemed problematic by, the Schrems II decision. Archer does not provide internet backbone services, but instead only carries traffic involving its own customers. To date, the U.S. Government has interpreted and applied FISA 702 upstream orders to only target market providers that have traffic flowing through their internet backbone and	

	that carry traffic for third parties (i.e., telecommunications carriers). EO 12333 contains no authorization to compel private companies to disclose personal data to US authorities. Furthermore, under FISA 702, an independent court is required to direct specific authority in relation to the type of foreign intelligence data acquisition. In accordance with the U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II whitepaper from September 2020, "ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data."	
What is Archer's practical experience dealing with government access requests in the US?	The EDPB Recommendations allow for the transfer impact assessment to take into account the "relevant prior instances of requests received from public authorities". Archer has never received any requests for access to personal data under Section 702 FISA. We are also not aware of any direct access to personal data under EO 12333.	
What is the impact of the recent signing of Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities (EO 14086)	The signing of the Executive Order provides binding safeguards which limit the U.S. intelligence authorities' access to data in accordance with what is **necessary and proportionate** to protect national security. It also contains the establishment of independent and impartial redress mechanism, review courts which shall	Note that the EU and EEA member states have been deemed as qualifying states that can benefit from EO 14086, in particular which ensures that EU and EEA citizens will be able to seek redress via the Office of the Director of National Intelligence ("ODNI") Civil Liberties Protection Officer ("CLPO"), and ultimately the U.S. Data Protection Review Court.

	investigate and address complaints concerning data access exercised by U.S. national security authorities. The impact of the signing of this EO is to both directly address two of the core issues raised in Schrems II i.e access to Personal Data is necessary and proportionate to what is required by national security law, and establishing an independent mechanism for challenging such access.	
EU Commission approves Adequacy Decision	EU Commission approves EU – US Data Privacy Framework as providing essentially equivalent Data Protection safeguards, and approves an adequacy decision based on this. In order to use the Adequacy Decision by the EU Commission for EU – US data transfers, organizations must update their current privacy programs to address the substantive and procedural requirements of DPF as well as self-certify with the US Department of Commerce. However, the Adequacy decision bears significant relevance in relation to applying the application of the Standard Contractual Clauses, because it validates that the DPF, as now supplemented with the additional safeguards implemented by EO 14086, validates the position that the application of EO14086 allows for essential equivalence in relation to EU Data protection laws.	An essential element of this adequacy approval were the commitments made in Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, which addressed the issues arising from the Schrems II decision (Refer to Question What is the impact of the recent signing of Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities above for further context on this).
Does the Cloud Act have any impact on transfers of Personal Data?	The CLOUD Act only permits U.S. government access to data in criminal investigations after obtaining a warrant approved by an	More information may be obtained here.

	independent court based on probable cause of a specific criminal act. The CLOUD Act does not allow U.S. government access in national security investigations, and it does not permit bulk surveillance	

Transfers to Australia		
Question	**Answer**	**Notes**
Are there any laws in Australian that enable government authorities to access personal in a manner which would impinge on the effectiveness of the provisions of the SCCs?	Archer is not aware of anything in the local laws and practices of the legal or regulatory regime in Australia that would, in practice, impinge on the ability to rely on the EU SCCs as an adequate transfer mechanism. Laws which relate to access to personal data by public authorities generally do not permit such access from private companies without effective safeguards and procedures, including a court order or warrant. Further, individuals have enforceable rights by way of legal remedies to seek judicial challenge. In theory, there are laws in Australia that relate to ability of governmental authorities to compel companies to disclose data, such as the Crimes Act 1914 (Cth) and the Criminal Code Act 1995 (Cth); the Surveillance Devices Act 2004 (Cth); and the Telecommunications (Interception and Access) Act 1979 (Cth) and Part 15 of the Telecommunications Act 1997 (Cth). However, in practice Archer has never received any request under any of the above referenced laws, and	

	given the purpose of those laws, it is highly unlikely for a commercial user of a business to business SaaS solution to be the subject of such a request.	

Transfers to India		
Question	**Answer**	**Notes**
Are there any laws in India that enable government authorities to access personal in a manner which would impinge on the effectiveness of the provisions of the SCCs?	The Information Technology Act 2000 applies to almost all businesses in India and can, in certain limited circumstances, permit government agencies to access information stored in a computer resource, and contains sanctions relating to foreign Surveillance. However, while the act grants the government the power to monitor and collect information, it can only do so in the interests of the "*sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence*". The legislative threshold to enable such access, therefore, is set very high, and in addition, in the event of such access, a data subject has direct recourse under Indian Law (see note in next column). The purpose limitation that this creates means that the risk of any such access is very low. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules):	Similar to the position which the European Convention on Human Rights imposes in the EU, at Article 8, India has recognized the right to Privacy by the Supreme Court* in India and have interpreted that this is a fundamental right guaranteed under the Constitution. Crucially, this also applies to non-citizens meaning that one of the core issues identified in Schrems II (adequate redress mechanisms by the data subject) is not an issue for such cases in India. *These rights were acknowledged by the Supreme Court of India in the case of Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018.

	Under this Act, Sensitive personal data or information may be shared without the data subjects' consent, only if such activity is mandated under law for verification of identity, prevention, detection and investigation purposes, including cyber incidents, prosecution and punishment of offences. Such data sharing activity would require the government agency to send a request in writing to the data controller/data processor stating the purpose of seeking such disclosure. **Indian Telegraph Act, 1885:** Section 5(2) of the Act confers upon the Indian government the right to conduct surveillance through telegraph lines, however, this is limited to circumstances of public emergency or in the interests of public safety. There are also procedural and due process restrictions under the Act. **Code of Criminal Procedure, 1973:** Grants courts the power to issue a search warrant in connection with criminal proceedings.	
Do any of the referenced laws actually impinge on Archer's ability to meet it's obligations under the SCC's?	There are various surveillance and interception laws referenced above in respect of Indian authorities ability to carry out investigations and access personal data. However, access to such data is, as noted above, limited to very specific purposes which are highly unlikely to arise in the context of the nature of	

	Services that Archer provides	

Step 4 and Step 5: Identify and apply the technical, contractual and organizational measures applied to protect the transferred data.

Technical Measures

Technical and organizational security measures in Archer's compliance programs include the following:

Refer to the Archer Information Security Provisions located at:
https://www.archerirm.com/company/standard-form-agreements

Contractual Measures:

1. Disclosure to third parties. Archer contractually agrees that it is not permitted to disclose Personal Data to any party other than those identified in Archer's Data Processing Addendum (located here: https://www.archerirm.com/company/standard-form-agreements). In particular, while Archer may be obligated to disclose Personal Data as required by applicable laws; however, to the extent that this arises Archer must, unless otherwise prohibited by law, inform the Customer in advance of making any disclosure of Personal Data and will reasonably cooperate with Customer to limit the scope, proportionality, and duration of such requested disclosure to what is strictly necessary or legally required.
2. Contractual provisions with Sub-processors. Archer flows through the same contractual provision referenced above in Section 1 to the 'Contractual Measures' in its contracts with its Sub processors.
3. Technical and Organizational measures. Archer contractually commits to meeting the technical and organizational measures that are specified in its Data Processing Addendum, and as set out in the 'Technical Measures' section above.
4. Standard Contractual Clauses obligations. Archer, and its Sub processors, are obligated in accordance with the provisions of the EU SCCs, which includes an obligation to notify customers if Archer is subject to a request for government access to personal data from a government authority. Archer is further obligated to review the legality of such a request.

Organizational Measures

1. Testing. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing are as follows:
2. Corporate security policies are reviewed at least annually, with final review/approval provided by the Chief Information Security Officer.
3. Employee Training. Appropriate employee training in place on processing of Personal Data and adherence to applicable laws and regulations as well as internal policies.
4. Background Checks. Jurisdiction based background checks are performed on all employees before hiring.
5. Access Requests. All requests received from third parties, including government bodies, for access to Personal Data must be reviewed by both the Risk Management Office and Legal, in order to ensure the validity of the request, where appropriate to challenge the request, and also to appropriately manage communications with customers, where applicable.

6. Vendor management process. Archer carries out robust due diligence procedures before onboarding any Vendors (Subprocessors) to ensure such Vendors are compatible with the manner in which Archer expects its supply chain to operate its business, ensuring responsible business practices and high standards of ethical behaviour. In particular, Archer ensures that, in engaging Subprocessors, it can continue to comply with its obligations in customer contracts.

Step 6: Re-evaluate at appropriate intervals

Archer will review and, if necessary, reconsider the risks involved to address changing data privacy regulations and / or local laws and practices of applicable importing countries.