Sinch Email
Transfer Impact Assessment

Fraud and reputation monitoring management

Data importer name: **Sinch Email ("data importer")**

Date of assessment: **July 7, 2022**

The purpose of this document is to assist Sinch assess whether the transfer of personal data originating from the European Economic Area, Switzerland and United Kingdom (collectively, "Europe") to the data importer will ensure an essentially equivalent level of protection and the supplementary measures that the data importer has implemented to ensure that such data remains protected in accordance with European law (including the GDPR).

In particular, this document describes the legal regimes applicable to the Fraud and reputation management department at the Sinch Email in the United States, the safeguards it puts in place in connection with transfers of customer personal data from Europe, and Sinch Email's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

Sinch Email is the Developer & Email business unit of Sinch. This business unit comprises of the brands Mailgun, Mailjet, Email on Acid and InboxReady.

Part 1: Know Your Transfers		
Details of the data importer		
1.	Name and address	Sinch Email US headquarters: 112 E Pecan St. Ste 1135. San Antonio, TX. 78205 EU headquarters: 4, rue Jules Lefebvre 75009 Paris, France Member of Company Group: Sinch AB, Lindhagensgatan 74 - 112 18 Stockholm, Sweden
2.	Contact persons	Dan Ross, Sr. Manager, Risk & Compliance Darine Fayed, General Counsel & DPO

3.	Nature of business	Fraud and reputation management department		
Details of the transfer				
4.	Will this be a one-off transfer or an ongoing series of transfers?	☐ One-off	☒ Ongoing	
5.	Will the data importer act as a controller or processor of the personal data?	☐ Controller	☒ Processor	
6.	What services does the data importer provide?	Sinch Email sends e-mails on behalf of our customers. The fraud and reputation management department monitors customer accounts and activities to protect its forums, websites, portals and the customer data within these portals against threats and fraud.		
7.	Where will the data importer access or otherwise process the data?	**Europe**	**Adequate territories**	**ROW**
		☒ European Economic Area[1] ☐ Switzerland ☐ United Kingdom	☐ Andorra ☐ Argentina ☐ Canada ☐ Faroe Islands ☐ Guernsey ☐ Israel ☐ Isle of Man ☐ Japan ☐ Jersey ☐ New Zealand ☐ Uruguay	☒ United States ☐ China ☐ Russia ☐ South Korea ☐ Singapore ☐ Brazil ☐ Other (please specify):

[1] This includes Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden, as well as Iceland, Liechtenstein and Norway

8.	Will the data importer onward transfer the data to other third parties? An onward transfer will take place if the data is further shared with or otherwise processed (e.g. accessed) by a third party (e.g., affiliate, partner or service provider), whether the third party is acting as a controller, processor or sub-processor.	☐ Yes ☒ No		
		Third party recipient name	**Purpose of transfer**	**Location of processing**
		Adyen	Monitoring payments and transactions	EU
Details of the data				
9.	What categories of data will be transferred?	☒ Contact information (name, email address) ☒ Online identifiers (IP address, customer ID number) ☒ Financial information (credit card transactions) ☐ Sensitive information ☐ Device information (e.g., operating system, language preferences) ☐ Internet or other online data (e.g., browsing or search history) ☐ Health information ☐ Geolocation data (e.g., IP address) ☐ Other (please specify): Click or tap here to enter text.		
10.	Does the data include communications contact or content information?	☒ Yes ☐ No		
		Contact information	**Content information**	
		☐ Telephone numbers ☒ Email addresses ☐ Social media contact information ☐ Physical addresses ☐ Other (please specify): Click or tap here to enter text.	☐ Telephone content ☒ Email content ☐ Online messages or communications ☐ Social media communications ☐ Other (please specify): Click or tap here to enter text.	

11.	Does the data include sensitive data?	☐ Yes ☒ No	
		Special category data	**Other sensitive information**
		☐ Health data ☐ Biometric data ☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Genetic data ☐ Data about sex life or sexual orientation	☐ Banking, financial or payment information ☐ Social security or national insurance information ☐ Passport or government-issued ID ☐ Data about criminal convictions or offences ☐ Other (please specify): Click or tap here to enter text.
12.	How many data subjects' personal data will be transferred? If it is impossible to estimate numbers due to volume, please reply "Large scale transfer".	☒ Large Scale Transfer Monitoring of account sign ups, email messages sent, credit card transactions	

Where Sinch Email processes personal data governed by European data protection laws as a data processor (on behalf of our customers), Sinch Email complies with its obligations under its Data Processing Addendum available here. The Sinch Email DPA incorporates the SCCs as per the EU Commission decision of June 2021 and provides the following additional information:

details and scope of the customer personal data processing (paragraph 3);

description of Sinch Email's security measures (Annex 2); and,

list of all of our data subprocessors (Annex 3).

Part 2: Identify the transfer tool relied upon		
13.	What transfer tool will be used to transfer data to the data exporter?	☐ Adequacy decision

		☒ Standard Contractual Clauses ("SCCs") ☐ Binding Corporate Rules ☒ Supplemental technical and organisational measures ☐ Other (please specify): Click or tap here to enter text.

Where personal data originating from Europe is transferred to Sinch Email in the US, Sinch Email relies upon the SCCs to provide an appropriate safeguard for the transfer, as well as any supplemental measures as deemed necessary to fully protect the personal data. Please see Annex 2 of our DPA available here for a full list of our TOMs.

Supplemental measures: Access control and restrictions to only requisite reputation team employees (restriction on access, additional okta sign in recommended)

Part 3: Assess whether the transfer tool relied upon is effective in light of the circumstances of the transfer		
14.	Are you aware of any laws in the destination territory that permit public authorities to intercept or access personal data in a manner that does not ensure an essentially equivalent level of protection to that guaranteed under European law?	☒ Yes ☐ No FISA Section 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. Executive Order 12333 authorizes US 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.
15.	Are you potentially subject to such security and surveillance laws? For example, if you are based in the US are you subject to Section 702 of the Foreign Intelligence Surveillance Act (FISA) or Executive Order 12333?	☒ Yes ☐ No ☐ We are under a legal obligation not to answer this question FISA, EO 12333 and other US surveillance laws apply as we use a Cloud service provider in the US. As per our privacy policy, Sinch Email will protect personal data wherever possible and will challenge any unlawful requests. Feel free to read more information from our subprocessor here on how they respond to government requests.
16.	Have you received any requests from public authorities for access to personal data or become aware of any direct access in the past?	☐ Yes ☒ No ☐ We are under a legal obligation not to answer this question If yes, please explain: Sinch Email has not received any FISA or EO 12333 requests to date. Sinch Email has received preservation requests, and requests related to criminal and cyber crime proceedings from EU and US authorities. Please see our Privacy policy on how we respond to these requests.

17.	Is there a good reason to believe that such security and surveillance laws will not be applied to the transferred data and/or data importer in practice?	☐ Yes ☒ No If yes, please explain with reference to any objective and publicly available sources of information that may support this belief: 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*." 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. The US Cloud Act only permits US government access to data in criminal investigations after obtaining a warrant approved by an independent court based on probable cause of a specific criminal act. No bulk surveillance is permitted.
Part 4: Identify the supplementary measures applied to protect the transferred data		
Technical measures		
18.	Do you encrypt data at rest?	☒ Yes ☐ No AES-256 inside databases
19.	Do you encrypt data in transit?	☒ Yes ☐ No TLS 1.2
20.	Do you take any other measures to pseudonymise the data before the transfer (e.g. hashing)?	☐ Yes ☒ No
21.	Are you considered a protected recipient? A "protected recipient" means that you are specifically protected by the laws of the destination territory, e.g. medical or legal confidentiality.	☐ Yes ☒ No If yes, please provide more detail: Click or tap here to enter text.
22.	Do you process the data using secure multi-party computation ("MPC")?	☐ Yes ☒ No If yes, please provide more detail:Click or tap here to enter text.
23.	Do you offer data hosting in the EEA?	☒ Yes ☐ No Germany and Belgium (EU datacenters) are an option if the Customer chooses

24.	Do you apply any other technical measures to protect the data?	☒ Yes ☐ No These can be found throughout the SOC 2 report and as part of our ISO27001 and 27701 certification management. Data protection is very important, and everything from Asset Inventory, classification, release and change management, Business Continuity, backups, and operational security is included as part of data protection.
Contractual measures		
25.	Are you required under the contract with the data exporter to implement any of the technical measures described above?	☒ Encryption at rest ☒ Encryption in transit ☐ Pseudonymisation before transfer ☐ Protected recipient ☐ Secure multi-party computation ("MPC") ☐ Other (please specify): Click or tap here to enter text.
26.	Are you required under the contract with the data exporter to notify the data exporter of any access requests you receive from public authorities or provide transparency reports regarding access requests?	☒ Yes ☐ No Data subject deletion requests come in, and these are forwarded to Customer to purge customer sending lists. Sinch Email can ensure backups are snapshotted with old backups deleted to ensure data is purged.
27.	Are you required under the contract with the data exporter to take specific action if you receive any access requests from public authorities?	☒ Yes ☐ No Actions to challenge access: Under the SCCs, Sinch Email is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.
Organisational measures		
28.	Do you have an internal policy regarding government access requests?	☒ Yes ☐ No These are reviewed by the Legal team individually before taking any sort of action. Under the SCCs, Sinch Email is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful. Where possible, the customer will be notified.
29.	Do you publish transparency reports or summaries regarding governmental access requests?	☐ Yes ☒ No Sinch Group intends to publish transparency reports, and Sinch Email will be included under its scope.

30.	Do you have effective (e.g., contractual) controls in place in relation to onward transfers?	☒ Yes ☐ No SCCs and supplemental measures are in place with all our vendors (Please refer to Annex 2 and Annex 3 of the Sinch Email DPA available here).
31.	Have you implemented any other organizational measures to ensure the data remains protected to an essentially equivalent standard?	☐ Yes ☒ No More information can be found at https://www.mailgun.com/gdpr/
Part 5: Procedural steps necessary to implement effective supplementary measures		
32.	Do you need to take any additional procedural steps to implement effective supplementary measures, in order to ensure that the data remains protected to an essentially equivalent standard?	☐ Yes ☒ No In light of the information provided in this document, including Sinch Email's practical experience dealing with government requests and the technical, contractual, and organizational measures Sinch Email has implemented to protect customer personal data, Sinch Email 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 SCCs (as "data importer") or to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.
Part 6: Re-evaluate the assessment at appropriate intervals		
33.	Will you inform the data exporter of any changes in the circumstances of the transfer or the laws and practices that apply in the destination territory that may affect the outcome of this assessment?	☒ Yes ☐ No Sinch Email will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of Europe.