SINCH EMAIL

Data Processing Addendum

This Data Processing Addendum (this "**DPA**") forms part of Sinch Email's Terms of Service (the "**Principal Agreement**") by and between Sinch Email and the Customer and is subject to the Principal Agreement. Sinch Email is the Developer & Email business unit of Sinch and comprises of the brands Mailgun, Mailjet, Email on Acid and InboxReady.

1. Definitions. For the purposes of this DPA, capitalized terms shall have the following meanings. Capitalized terms not otherwise defined shall have the meaning given to them in the Principal Agreement.

(a) **"Customer's Personal Data**" means any personal data that is processed by Sinch Email on behalf of the Customer to perform the Services under the Principal Agreement.

(b) **"Applicable Data Protection Laws"** means the GDPR, as transposed into domestic legislation of each Member State (and the United Kingdom) and as amended, replaced or superseded from time to time, and laws implementing, replacing or supplementing the GDPR and all laws applicable to the collection, storage, processing, and use of Customer's Personal Data, including the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq.

(c) "**GDPR**" means EU General Data Protection Regulation 2016/679.

(d) **"Sinch Email Infrastructure"** means (i) Sinch Email's physical facilities; (ii) hosted cloud infrastructure; (iii) Sinch Email's corporate network and the non-public internal network, software, and hardware necessary to provide the Services and which is controlled by Sinch Email; in each case to the extent used to provide the Services.

(e) "**Restricted Transfer**" means a transfer of the Customer's Personal Data from Sinch Email to a sub-processor where such transfer would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Data Protection Laws) in the absence of appropriate safeguards required for such transfers under Applicable Data Protection Laws.

(f) "**Services**" means the services provided to the Customer by Sinch Email pursuant to the Principal Agreement.

(g) "**Standard Contractual Clauses**" means the latest version of the standard contractual clauses for the transfer of personal data to processors established in third countries under the GDPR (the current version as at the date of this DPA is as annexed to European Commission Decision 2021/914 (EU) of June 4, 2021).

(h) "**UK Addendum**" means the United Kingdom Addendum (International Data Transfer Addendum to the EU Commission Standard Contractual Clauses) set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

(i) The terms "**consent**", "**controller**", "**data subject**", "**Member State**", "**personal data**", "**personal data breach**", "**processor**", "**sub processor",** "**processing**", "**supervisory authority**" and "**third party**" shall have the meanings ascribed to them in article 4 of the GDPR.

2. Compliance with Applicable Data Protection Laws

(a) Sinch Email and the Customer shall each comply with the provisions and obligations imposed on them by the Applicable Data Protection Laws and shall procure that their employees, agents and contractors observe the provisions of the Applicable Data Protection Laws.

3. Details and Scope of the Processing

(a) The Processing of the Customer's Personal Data within the scope of the Agreement shall be carried out in accordance with the following stipulations and as required under Article 28(3) of the GDPR. The parties may amend this information from time to time, as the parties may reasonably consider necessary to meet those requirements.

(i) **Subject matter and duration of the processing of Personal Data:** The subject matter and duration of the processing of the Personal Data are set out in the Principal Agreement.

(ii) **The nature and purpose of the processing of Personal Data:** Under the Principal Agreement, Sinch Email provides certain email and sms services to the Customer which involves the processing of personal data. Such processing activities include (a) providing the Services; (b) the detection, prevention and resolution of security and technical issues; and (c) responding to Customer's support requests.

(iii) **The types of Personal Data to be processed:** The personal data submitted, the extent of which is determined and controlled by the Controller in its sole discretion, includes name, email, telephone numbers IP address and other personal data included in the contact lists and message content.

(iv) **The categories of data subjects to whom the Personal Data relates:** Senders and recipients of email and sms messages.

(b) Sinch Email shall only process the Customer's Personal Data (i) for the purposes of fulfilling its obligations under the Principal Agreement and (i) in accordance with the documented instructions described in this DPA or as otherwise instructed by the Customer from time to time. Such Customer's instructions shall be documented

in the applicable order, services description, support ticket, other written communication or as directed by Customer using the Services (such as through an API or control panel).

(c) Where Sinch Email reasonably believes that a Customer instruction is contrary to the provisions of the Principal Agreement or this DPA, or that it infringes the GDPR or other applicable data protection provisions, it shall inform the Customer without delay. In both cases, Sinch Email shall be authorized to defer the performance of the relevant instruction until it has been amended by Customer or is mutually agreed by both Customer and Sinch Email.

(d) Customer is solely responsible for its utilization and management of Personal Data submitted or transmitted by the Services, including: (i) verifying recipient's addresses and that they are correctly entered into the Services (ii) reasonably notifying any recipient of the insecure nature of email as a means of transmitting Personal Data (as applicable), (iii) reasonably limiting the amount or type of information disclosed through the Services (iv) encrypting any Personal Data transmitted through the Services where appropriate or required by applicable law (such as through the use of encrypted attachments, PGP toolsets, or S/MIME). When the Customer decides not to configure mandatory encryption, the Customer acknowledges that the Services may include the transmission of unencrypted email in plain text over the public internet and open networks. Information uploaded to the Services, including message content, is stored in an encrypted format when processed by the Sinch Email Infrastructure.

4. Controller and Processor

(a) For the purposes of this DPA, the Customer is the controller of the Customer's Personal Data and Sinch Email is the processor of such data, except when the Customer acts as a processor of the Customer's Personal Data, in which case Sinch Email is a sub-processor.

(b) Sinch Email shall at all times have in place an officer who is responsible for assisting the Customer (i) in responding to inquiries concerning the Data Processing received from Data Subjects; and, (ii) in completing all legal information and disclosure requirements which apply and are associated with the Data Processing. The Data Protection Officer may be contacted directly at privacy@mailgun.com.

(c) The Customer warrants that:

(i) The processing of the Customer's Personal Data is based on legal grounds for processing, as may be required by Applicable Data Protection Laws and that it has made and shall maintain throughout the term of the Principal Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by Applicable Data Protection Laws with respect to Sinch Email's processing of the Customer's Personal Data under this DPA and the Principal Agreement;

(ii) it is entitled to and has all necessary rights, permissions and consents to transfer the Customer's Personal Data to Sinch Email and otherwise permit Sinch Email to process the Customer's Personal Data on its behalf, so that Sinch Email may lawfully use, process and transfer the Customer's Personal Data in order to carry out the Services and perform Sinch Email's other rights and obligations under this DPA and the Principal Agreement;

(iii) it will inform its Data Subjects about its use of Processors in Processing their Personal Data, to the extent required under Applicable Data Protection Laws; and,

(iv) it will respond in a reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data, and to give appropriate instructions to the Processor in a timely manner.

5. Confidentiality

(a) Sinch Email shall ensure that each of its, and sub-processors', personnel that is authorized to process the Customer's Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality and are trained with the relevant security and Data Protection requirements.

6. Technical and Organizational Measures

(a) Sinch Email shall, in relation to the Customer's Personal Data, (a) take and document, as appropriate, reasonable and appropriate measures required pursuant to Article 32 of the GDPR in relation to the security of the Sinch Email Infrastructure and the platforms used to provide the Services as described in the Principal Agreement, and (b) on reasonable request at the Customer's cost, assist the Customer in ensuring compliance with the Customer's obligations pursuant to Article 32 of the GDPR.

(b) Sinch Email’s internal operating procedures shall comply with the specific requirements of an effective Data Protection management.

7. Data Subject Requests

(a) Sinch Email provides specific tools in order to assist customers in replying to requests received from data subjects. These include our APIs and interfaces to search event data, suppressions, and retrieve message content. When Sinch Email receives a complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to Applicable Data Protection Laws) related to the Customer's Personal Data directly from data subjects Sinch Email will notify the Customer within fourteen (14) days from the receipt of the complaint, inquiry or request. Taking into account the nature of the processing, Sinch Email shall assist the Customer, by appropriate technical and organizational measures, insofar as this

is reasonably possible, for the fulfillment of the Customer's obligation to respond to requests for exercising such data subjects' rights.

8. Personal Data Breaches

(a) Sinch Email shall notify the Customer without undue delay once Sinch Email becomes aware of a personal data breach affecting the Customer's Personal Data. Sinch Email shall, taking into account the nature of the processing and the information available to Sinch Email, use commercially reasonable efforts to provide the Customer with sufficient information to allow the Customer at the Customer's cost, to meet any obligations to report or inform regulatory authorities, data subjects and other entities of such personal data breach to the extent required under Applicable Data Protection Laws.

9. Data Protection Impact Assessments

(a) Sinch Email shall, taking into account the nature of the processing and the information available, provide reasonable assistance to the Customer at the Customer's cost, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for the Customer to fulfill its obligations under Applicable Data Protection Laws.

10. Audits

(a) Sinch Email shall make available to the Customer on reasonable request, information that is reasonably necessary to demonstrate compliance with this DPA.

(b) Customer, or a mandated third party auditor, may upon written reasonable request conduct an inspection in relation to the Processing of the Customer’s Personal Data by Sinch Email and to the extent necessary according to Data Protections Laws and without interrupting Sinch Email’s business operations and ensuring confidentiality.

(c) The audit right as described in Paragraph 10(b) above will become applicable for the Customer, in case Sinch Email has not provided sufficient evidence of its compliance with the technical and organizational measures. Sufficient evidence includes providing either: (i) a certification as to compliance with ISO 27001, ISO 27701 or other standards implemented by Sinch Email (scope as defined in the certificate); or (ii) an audit or attestation report of an independent third party. An audit as described within this Paragraph 10 shall be carried out at the Customer's cost and expense.

11. Return or Destruction of the Customer's Personal Data

(a) The Customer may, by written notice to Sinch Email, request the return and/or certificate of deletion of all copies of the Customer's Personal Data in the control or possession of Sinch Email and sub-processors. Sinch Email shall provide a copy of the Controller's Data in a form that can be read and processed further.

(b) Within ninety (90) days following termination of the account, the Processor shall delete and/or return all Personal Data processed pursuant to this DPA. This provision shall not affect potential statutory duties of the Parties to preserve records for retention periods set by law, statute or contract. Sinch Email may retain electronic copies of files containing Customer's Personal Data created pursuant to automatic archiving or back-up procedures which cannot reasonably be deleted. In these cases, Sinch Email shall ensure that the Customer's Personal Data is not further actively processed.

(c) Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by the Customer.

12. Data Transfers

(a) The Standard Contractual Clauses and, if required, the UK Addendum, having Sinch Email act as data importer with the Customer acting as data exporter are incorporated as part of this DPA. If Sinch Email's arrangement with a sub-processor involves a Restricted Transfer, Sinch Email shall ensure that the onward transfer provisions of the Standard Contractual Clauses and/or UK Addendum are incorporated into the Principal Agreement, or otherwise entered into, between Sinch Email and the sub-processor. The Customer agrees to exercise its audit right in the Standard Contractual Clauses by instructing Sinch Email to conduct the audit set out in Paragraph 10.

(b) Controller acknowledges and agrees that, in connection with the performance of the Services under the Agreement, Processor may transfer Personal Data within its company group. These transfers are necessary to globally provide the Services, and are justified for internal administration purposes.

(c) For transfers of Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of Data Protection within the meaning of Data Protection Laws of the foregoing territories, to the extent such transfers are subject to Data Protection Laws and Regulations and in order to implement appropriate safeguards, the following safeguards are taken: (i) Standard Contractual Clauses as per European Commission's Decision 2021/914/EU of June 4, 2021, (2) UK Addendum, and (3) additional safeguards with respect to security measures including data encryption, data aggregation, separation of access controls and data minimization principles.

13. Sub-processing

(a) The Customer hereby authorizes Sinch Email to appoint sub-processors in accordance with this Paragraph 13 and Annex 1, subject to any restrictions in the Principal Agreement. Sinch Email will ensure that sub-processors are bound by written agreements that require them to provide at least the level of data protection

required of Sinch Email by this DPA. Sinch Email may continue to use those sub-processors already engaged as at the date of this DPA.

(b) Sinch Email shall give the Customer prior written notice of the appointment of any new sub-processor. If, within ten (10) business days of receipt of that notice, the Customer notifies Sinch Email in writing of any objections on reasonable grounds to the proposed appointment, Sinch Email shall not appoint that proposed sub-processor until reasonable steps have been taken to address the objections raised by the Customer and the Customer has been provided with a reasonable written explanation of the steps taken. If Sinch Email and the Customer are not able to resolve the appointment of a sub-processor within a reasonable period, either party shall have the right to terminate the Principal Agreement for cause.

(c) This paragraph does not apply to the following ancillary services, namely telecommunication services, postal or transport services, maintenance and user support tools. Mailgun shall, however, be obligated to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the Data protection and Data security of the Customer's Data even for these outsourced ancillary services.

(d) Sinch Email shall be responsible for the acts and omissions of any sub-processors as it is to the Customer for its own acts and omissions in relation to the matters provided in this DPA.

14. Governing law and jurisdiction

(a) The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

(b) This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

15. Order of precedence

(a) With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

16. Severance

(a) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision

shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

17. Termination

(a) This DPA and the Standard Contractual Clauses will terminate contemporaneously and automatically with the termination of the Principal Agreement.

(b) Any amendment or variation to this DPA shall not be binding on the Parties unless set out in writing and signed by authorised representatives of each of the Parties.

* * *

IN WITNESS WHEREOF, this DPA and the Annexes are entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Sinch Email

Signature: DocuSigned by: Anton Efimenko 984E9C30C3884AB...

Name: Anton Efimenko

Title: VP, Engineering

1/11/2023

The Customer

Signature:

Name:

Title:

Date Signed:

Signed by: 647DA8158167498...

Stephen Knott

Managing Director

11/25/2024

ANNEX 1

STANDARD CONTRACTUAL CLAUSES

With regard to the Standard Contractual Clauses the Parties agree that:

(a) Module 2 (Controller-to-Processor) will apply where Sinch Email acts as Customer's data processor; Module 3 (Processor-to-Processor) will apply where Sinch Email acts as Customer sub-processor. For each Module, where applicable:
(b) Clause 7 (Docking clause) is incorporated;
(c) For the purposes of Clause 9.a) (Use of sub-processors), Option 2: General written authorization shall apply. The data importer has the data exporter's general authorization for the engagement of sub-processors from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance;
(d) The optional wording in Clause 11 (Redress) on independent resolution bodies is not incorporated;
(e) For the purpose of Clause 13 (Supervision), CNIL, the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*) shall act as competent supervisory authority;
(f) Option 1 of Clause 17 (Governing law) shall apply and the laws of France shall govern the Standard Contractual Clauses;
(g) For the purposes of Clause 18 (Choice of forum and jurisdiction), the courts of France will resolve any dispute arising out of the Standard Contractual Clauses;
(h) Annex IA (List of Parties) and Annex IB (Description of Transfer) shall be completed using the information and details specified in the Principal Agreement and listed in Paragraph 3 of the DPA;
(i) Annex IB (Description of Transfer) shall be further completed by specifying that no sensitive data shall be transferred. The frequency of the transfer shall be continuous. For transfers to sub- processors, the subject matter, nature and duration of the processing shall be the same as that of the data importer;
(j) For the purpose of Annex IC, the competent supervisory authority in accordance with Clause 13 is CNIL, the French Data Protection Authority, (Commission Nationale de l'Informatique et des Libertés);
(k) For the purpose of Annex II, the Technical and organisational measures are described in Annex 2 of the DPA;
(l) For the purpose of Annex III, the List of Sub processors is inluded in Annex 3 of the DPA;
(m) where the Restricted Transfer is subject to the Regulation as it forms part of the law of England and Wales, Scotland and Northern Ireland (UK GDPR), the Standard Contractual Clauses shall incorporate the UK Addendum completed as follows:
    (i) For the purposes of Table 1, the start date is the the date of the DPA's signature and the Parties' details shall be completed using the information and details specified in the Principal Agreement;
    (ii) For the purposes of Table 2, the version of the Approved EU SCCs which the UK Addendum is appended to is the Standard Contractual Clauses as completed in accordance with this Annex 1, with the date being the effective date of this Addendum;

(iii) For the purposes of Table 3, the Appendix Information is as described in paragraphs (h) - (l) of this Annex 1; and,

(iv) For the purposes of Table 4, Mailgun as the Importer may end the UK Addendum when the Approved Addendum changes.

ANNEX 2

INFORMATION SECURITY - TECHNICAL AND ORGANIZATIONAL MEASURES

Where personal data is processed or used automatically, Sinch Email's internal organization ensures that it meets specific requirements of data protection by utilizing security best practices. In particular, Sinch Email implements the following measures to protect personal data or other sensitive data categories.

Physical Access Control

To prevent unauthorized persons from gaining access to data processing systems with which personal data is processed or used:

- Sinch Email leverages industry-leading data center and cloud infrastructure providers. Access to all data centers is strictly controlled. All data centers are equipped with 24x7x365 surveillance and biometric access control systems. Additionally, all providers have industry standard certifications.
- Data centers are equipped with at least N+1 redundancy for power, networking, and cooling infrastructure.
- Within a region, data processing occurs across at least three distinct availability zones. Services are designed to withstand the failure of an availability zone without customer disruption.

System Access Control

To prevent data processing systems from being used without authorization:

- Administrative access to Sinch Email systems and services follows the principle of least privilege. Access to systems is based on job role and responsibilities. Sinch Email utilizes unique usernames/identifiers that are not permitted to be shared or re-assigned to another person.
- VPN and multi-factor authentication is used for access to internal support tools and product infrastructure.
- Network access control lists (ACLs) and security groups are used to limit ingress and egress traffic from production infrastructure.
- Intrusion detection systems (IDS) are used to detect potential unauthorized access.
- Network protections have been deployed to mitigate the impact of distributed denial of service (DDoS) attacks.
- Onboarding and offboarding processes are documented and followed consistently to ensure access is properly managed to internal and externally hosted tools and systems. Where possible, third-party services leverage single sign-on (SSO) functionality which allows for centralized management and enforces multi-factor authentication.

Data Access Control

To ensure authorized users entitled to use data processing systems have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage:

- Sinch Email utilizes a password management system that enforces minimum password length, complexity, expiration time, and minimum last used.
- Employee workstations automatically lock after a prolonged period of inactivity. Systems log out users after a prolonged period of inactivity.
- Logs are centrally stored and indexed. Critical logs, such as security logs, are retained for at least one year.
- The Sinch Email patch management process ensures that systems are patched at least once every month. Monitoring, alerting, and routine vulnerability scanning occurs to ensure that all product infrastructure is patched consistently.
- Industry-standard antivirus software is utilized to ensure internal assets that access personal data are protected against known viruses. Antivirus software is updated regularly.
- Sinch Email utilizes firewall devices to segregate unwanted traffic from entering the network. A DMZ is utilized using firewalls to further protect internal systems protecting sensitive data.

Data Transmission Control

To ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport:

- Customer data is stored encrypted-at-rest through the use of AES-256 encryption on block devices.
- Customer backups are encrypted-in-transit and at rest using strong encryption.
- Sinch Email supports TLS 1.2 to encrypt network traffic between the client application and Sinch Email infrastructure.
- Sinch Email is alerted to encryption issues through periodic risk assessments and third-party penetration tests. Sinch Email performs third-party penetration tests on an annual basis, or as needed due to changes in the business.
- Sinch Email operates a bug bounty program, encouraging the responsible disclosure of vulnerabilities from community researchers.

Input Control

To ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed:

- Systems are monitored for security events to ensure quick resolution.
- Logs are centrally stored and indexed. Critical logs, such as security logs, are retained for at least one year. Logs can be traced back to individual unique usernames with timestamps to investigate nonconformities or security events.

Availability Control

To ensure personal data is protected from accidental destruction or loss:

- Account data is backed up at least daily. Incremental/point-in-time recovery is available for all primary databases. Backups are encrypted-in-transit and at rest using strong encryption.
- Sinch Email patch management process ensures that systems are patched at least once every month. Monitoring, alerting, and routine vulnerability scanning occurs to ensure that all product infrastructure is patched consistently.
- When necessary, Sinch Email patches infrastructure in an expedited manner in response to the disclosure of critical vulnerabilities to ensure system uptime is preserved.
- Customer environments are logically separated at all times. Customers are not able to access accounts other than those given authorization credentials for.

Certification/assurance of processes and products

To ensure internal IT and IT security governance and management as well as assurance of processes and products

- ISO 27001 certification
- ISO 27701 certification
- SOC 2 Type 2 report (Mailgun & Mailjet brands only)
- SOC 2 Type 1 report (Email on Acid brand only)

ANNEX 3

AUTHORIZED SUB-PROCESSORS AS OF THE DPA EFFECTIVE DATE

Infrastructure Sub-Processors			
Company	**Server Location**	**Description of Activities**	**Appropriate Safeguards for transfers**
Google Cloud Platform 70 Sir John Rogerson's Quay, Dublin 2, Ireland	Germany & Belgium (EU customers) USA (US customers)	Datacenters (Products: Mailgun, Mailjet & InboxReady)	SCCs Data encryption
Rackspace (AWS) One Fanatical Place San Antonio, TX 78218 USA	USA (US customers) Germany (EU customers)	Datacenters (All Products)	SCCs Data encryption
MacStadium 3525 Piedmont Road, Bldg 7 Atlanta, GA 30305	USA	Datacenters (Email on Acid)	SCCs Data encryption
Cyxtera 9180 Commerce Center Cir Highlands Ranch, CO 80129	USA	Datacenters (Email on Acid)	SCCs Data encryption
Support Sub-Processors			
Company	**Location**	**Description of Activities**	**Appropriate Safeguards for transfers**
Proxiad Bulgaria Tintyava 13b St., Fl. 4 Sofia 1113 - Bulgaria	Bulgaria	Ticket support functions TAM functions	EU law Data minimization
Sitel India Chandivali – Farm Road, Andheri East Mumbai 400072 India	India	Ticket support functions *(provide first response through ticketing system; no access to customer personal data*)	SCCs Data encryption Data minimization
Group Company Sub-Processors			
Company	**Headquarters**	**Description of Activities**	**Appropriate Safeguards for transfers**
Mailgun Technologies 112 E. Pecan Street #1135, San Antonio, Texas, 78205 USA	USA	Group company *(Administrative, billing, support and maintenance services)*	SCCs Data encryption Data minimization

Mailjet 4, rue Jules Lefebvre 75009 Paris, France	France	Group company	SCCs Data encryption Data aggregation
Sinch AB Lindhagensgatan 74 Stockholm, 112 18 Sweden	Sweden	Group company	SCCs Data encryption Data aggregation