Data Processing Agreement

This Data Processing Agrement ("**DPA**") amends the terms and forms part of the Agreement defined below by and between you ("**Customer**") and the applicable Cillco entity from which you are purchasing Cloud Products ("**Cillco**") and shall be effective on the later of (i) the effective date of the Agreement; or (ii) the date both parties execute this DPA in accordance with Section 1 below ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Company name:
Address:
Postal code and city:
Country:

(the Customer) acting as data controller

and

Cillco AS/Cillco Technology AS/Cillco Consulting AS
Brattørgata 5
7010 Trondheim
Norway

(Cillco) acting as data processor

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Instructions and Effectiveness

This DPA has been pre-signed on behalf of Cillco. To enter into this DPA, Customer must

a. be a customer of the Cillco Cloud Products
b. complete the signature block below by signing and providing all relevant information
c. send the completed and signed DPA to Cillco as a PDF to dataprotection@cillco.com

This DPA will only be effective (as of the Effective Date) if executed and submitted to Cillco accurately and in full accordance with Section 1. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

Customer signatory represents to Cillco that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

Notwithstanding expiry or termination of the Agreement, this DPA and any Standard Contractual Clauses (if applicable) will remain in effect until, and will terminate automatically upon, deletion by Cillco of all personal data covered by this DPA, in accordance with this DPA.

2. Definitions

In this DPA, the following terms shall have the following meanings:

a. "**Agreement**" means the contract in place between Customer and in connection with the purchase of Cloud Products by Customer;

b. "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in European Data Protection Law;

c. "**Applicable Data Protection Law**" means US Data Protection Law and European Data Protection Law that are applicable to the processing of Customer Personal Data under this DPA;

d. "**Customer Personal Data**" means any personal data provided by (or on behalf of) Customer to Cillco in connection with the Services, all as more particularly described in this DPA

e. "**EEA**" means the European Economic Area;

f. "**End Users**" means an individual you permit or invite to use the Cloud Products. For the avoidance of doubt: (a) individuals invited by your End Users, (b) individuals under managed accounts, and (c) individuals interacting with a Cloud Product as your customer are also considered End Users

g. "**European Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "EU GDPR"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act ("Swiss DPA").

h. "**Standard Contractual Clauses**" means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs")

i. "**Security Incident**" means any confirmed breach of security that leads to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of or access to Customer Personal Data processed by Cillco and/or its Sub-processors in connection with the provision of the Service. "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems

j. "**Services**" means the provision of the Cloud Products by Cillco to Customer pursuant to the Agreement

k. **"Special categories of data"** means any Customer Personal Data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) that is genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, and (iii) relating to criminal convictions and offences.

l. "**Sub-processor**" means any processor engaged by Cillco to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data. Sub-processors may include Colco's affiliates or other third parties.

m. "**CCPA**" means California Consumer Privacy Act.

3. Preamble

a. These Contractual Clauses (the Clauses) set out the rights and obligations of the Customer and Cillco, when processing personal data on behalf of the Customer.

b. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

c. In the context of the provision of Cloud Products, Cillco will process personal data on behalf of the Customer in accordance with the Clauses.

d. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

e. Two appendices are attached to the Clauses and form an integral part of the Clauses.

f. A description of the processing of personal data related to the Services, as applicable, is set out in Appendix A. The parties acknowledge and agree that the description of processing can be updated by Cillco from time to time to reflect new products, features or functionality comprised within the Services. Cillco will update relevant documentation to reflect such changes.

g. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

h. The Clauses shall not exempt Cillco from obligations to which Cillco is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

4. The rights and obligations of the Customer

The Customer is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

The Customer has the right and obligation to make decisions about the purposes and means of the processing of personal data.

The Customer shall be responsible, among other, for ensuring that the processing of personal data, which Cillco is instructed to perform, has a legal basis.

5. Cillco acts according to instructions

Cillco shall process the Customer Personal Data as a processor, as necessary to perform its obligations under the Agreement and strictly in accordance with the documented lawful instructions of Customer (as set forth in the Agreement, or in this DPA, or as directed by you through the Cloud Products) (the "**Permitted Purpose**"). Cillco shall not retain, use, disclose or otherwise process the Customer Personal Data for any purpose other than the Permitted Purpose except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law, and shall not "sell" the Customer Personal Data within the meaning of the CCPA or otherwise. Cillco shall promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law.

6. Confidentiality

Cillco shall ensure that any person that it authorizes to process Customer Personal Data (including Cillco's staff, agents and Sub-processors) (an "**Authorized Person**") shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process Customer Personal Data who is not under such a duty of confidentiality.

7. Security of processing

Cillco and, to the extent required under the Agreement, Customer shall implement appropriate technical and organizational measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with Cillco's security standards described in Appendix B ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Cillco may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

8. Use of sub-processors

Customer agrees that Cillco may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by Cillco and authorized by Customer are listed at https://www.cillco.com/legal-subprocessors. Cillco will: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Laws (and in substance, to the same standard provided by this DPA); and (ii) remain responsible to Customer for the performance of such Sub-processor's data protection obligations under such terms.

Cillco shall (i) make available an up-to-date list of the Subprocessors it has appointed upon written request from Customer; and (ii) notify Customer if it adds any new Sub-processors at least fourteen (14) days' prior to allowing such Subprocessor to process Customer Personal Data. Customer must subscribe to receive notice of updates to the list of Sub-processors, using the following link https://www.cillco.com/legal-subprocessors. Customer may object in writing to Cillco's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the Agreement (including this DPA) for convenience.

9. Transfer of data to third countries or international organizations

a. Any transfer of personal data to third countries or international organizations by Cillco shall only occur on the basis of documented instructions from the Customer and shall always take place in compliance with Chapter V GDPR.

b. In case transfers to third countries or international organizations, which Cillco has not been instructed to perform by the Customer, is required under EU or Member State law to which Cillco is subject, Cillco shall inform the Customer of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

c. Without documented instructions from the Customer, Cillco therefore cannot within the framework of the Clauses:

   i. transfer personal data to a Customer or a data processor in a third country or in an international organization

   ii. transfer the processing of personal data to a sub-processor in a third country

   iii. have the personal data processed in by Cillco in a third country

d. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

10. Assistance to the Customer

a. Cillco shall provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party, in each case in respect of Customer Personal Data that Cillco processes on Customer's behalf;

b. In the event that any request, correspondence, enquiry or complaint (referred to under paragraph (a) above) is made directly to Cillco, Cillco acting as a processor shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so, and instead, after being notified by Cillco, Customer shall respond. If Cillco is legally required to respond to such a request, Cillco will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so; and

c. To the extent Cillco is required under Applicable Data Protection Law, Cillco shall (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

11. Notification of personal data breach

In case of any personal data breach, Cillco shall, without undue delay after having become aware of it, notify the Customer of the personal data breach.

Cillco's notification to the Customer shall, if possible, take place within 24 hours after Cillco has become aware of the personal data breach to enable the Customer to comply with the Customer's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
In accordance with Clause 9 (a), Cillco shall assist the Customer in notifying the personal data breach to the competent supervisory authority, meaning that Cillco is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the Customer's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

12. Erasure and return of data

On termination of the provision of personal data processing services, Cillco shall be under obligation to delete all personal data processed on behalf of the Customer and certify to the Customer that it has done so unless Union or Member State law requires storage of the personal data.

Cillco commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

13. Audit and inspection

a. Customer acknowledges that Cillco is regularly audited by independent third-party auditors and/or internal auditors. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Cillco, Cillco shall:

   i. supply (on a confidential basis) a summary copy of its audit report(s) ("Report") to Customer, so Customer can verify Cillco's compliance with the audit standards against which it has been assessed, and this DPA; and

   ii. provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security and audit questionnaires, that are necessary to confirm Cillco's compliance with this DPA, provided that Customer shall not exercise this right more than once per calendar year.

b. Only to the extent Customer cannot reasonably satisfy Cillco's compliance with this DPA through the exercise of its rights under 13(a) above, where required by Applicable Data Protection Law or the Standard Contractual Clauses, Customer and its authorized representatives may conduct audits (including inspections) during the term of the Agreement to establish Cillco's compliance with the terms of this DPA, on the condition that Customer and its authorized representatives have entered into an applicable non-disclosure agreement with Cillco. Notwithstanding the foregoing, any audit (or inspection) must be conducted during Cillco's regular business hours, with reasonable advance notice (which shall not be less than 45 calendar days) and subject to reasonable confidentiality procedures. Any assistance from Cillco during such an audit is billable to the Customer. Such audit (or inspection) shall not require Cillco to disclose to Customer or its authorized representatives, or to allow Customer or its authorized representatives to access:

c. any data or information of any other Cillco customer (or such customer's End Users);

   iii. any Cillco internal accounting or financial information;

   iv. any Cillco trade secret;

   v. any information that, in our reasonable opinion could: (1) compromise the security of our systems or premises; or (2) cause us to breach our obligations under Applicable Data Protection Law or our security, confidentiality and or privacy obligations to any other Cillco customer or any third party; or

   vi. any information that Customer or its authorized representatives seek to access for any reason other than the good faith fulfilment of Customer's obligations under the Applicable Data Protection Law and Cillco's compliance with the terms of this DPA.

   vii. An audit or inspection permitted in compliance with Section 13(b) shall be limited to once per calendar year, unless (1) Cillco has experienced a Security Incident within the prior twelve (12) months which has impacted Customer Personal Data; or (2) Customer is able to evidence an incidence of Cillco's material noncompliance with this DPA.

14. Miscellaneous

Customer acknowledges and agrees that as part of providing the Cloud Products and services, Cillco has the right to use data relating to or obtained in connection with the operation, support or use of the Cloud Products for its legitimate internal business purposes, such as to support billing processes, to administer the Cloud Products, to improve, benchmark, and develop Cillco products and services, to comply with applicable laws (including law enforcement requests), to ensure the security of the Cloud Products and to prevent fraud or mitigate risk. To the extent any such data is personal data, Cillco warrants and agrees that:

a. it will process such personal data in compliance with Applicable Data Protection Law and only for the purposes that are compatible with those described in this Clause 14; and

b. it will not use such personal data for any other purpose or disclose it externally unless it has first aggregated and anonymized the data, so it does not identify the Customer or any other person or entity.

Through use of the Cloud Products, as further described in the Agreement, Customer or Customer's End Users, as applicable, may elect to grant third parties visibility to data or content (which may include Customer Personal Data). Customer understands that user profile information for the Cloud Products may be publicly visible. Nothing in this DPA prohibits Cillco from making Customer's data or content (which may include personal data) visible to third parties consistent with this paragraph, as instructed by Customer or Customer's End Users through the Cloud Products.

15. Commencement and termination

The Clauses shall become effective on the date of both parties' signature.

The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Customer pursuant to Clause 12, the Clauses may be terminated by written notice by either party.

Signature

On behalf of the Customer

Customer name (Required)	_____
Name (Required)	_____
Position/Title	_____
Date (Required)	_____
Signature (Required)	_____

On behalf of Cillco

Name:	Yngve Tronstad
Position/Title:	Chairman of the Board
Date:	01.05.2022
Signature (Required)	_____

16. Customer and data processor contacts/contact points

c. The parties may contact each other using the following contacts/contact points:

d. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Customer		**Cillco**
Name	Yngve Tronstad	Data Protection Point of Contact:
Position/Title		Yngve Tronstad
Phone		dataprotection@cillco.com
E-mail		

Appendix A - Information about the processing

List of Parties

Data Exporter	**Data Importer**
Name: Customer	Name: Cillco
Address / Email Address: As provided for in the DPA	Address / Email Address: As provided for in the DPA
Contact Person's Name, position and contact details: As provided for in the DPA	Contact Person's Name, position and contact details: As provided for in the DPA
Activities relevant to transfer: See below	Activities relevant to transfer: See below
Role: See below	Role: See below

Description of Processing / Transfer

The parties acknowledge that Cillco's processing of personal data will include all personal data submitted or uploaded to the Services by Customer from time to time, for the purpose of, or otherwise in connection with, Cillco providing the Services to Customer. Set out below are descriptions of the processing/transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or may be supplemented pursuant to Section 2 (f) of the DPA.

Cillco account profile (Identity)	
Categories of data subjects	Customers, customers' employees, customers' collaborators

Categories of personal data transferred	• User Account Information
	• Cillco identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification
	• Employment Information, including:
	  ○ Job title / role
	  ○ Office / location
	  ○ Company/Organization

Controller/ Processor roles	Controller (Customer) to Processor (Cillco)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • To maintain and display user profiles during collaboration, authenticate users, and manage access control and user permissions.
Purpose of the data transfer	Providing the products and services, including: • To allow collaboration and maintain proper access controls and user permissions.
Duration of processing	Data will be deleted 15 days (for evaluation sites) or 60 days (for paid subscription sites) after a customer has been unsubscribed due to missed payment for a Cillco product subscription or if a customer cancels their Cillco product subscription.

Cillco Applications	
Categories of data subjects	Customers, customers' employees, customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Cillco identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification
	• Employment Information, including:
	  ○ Job title / role
	  ○ Office / location
	  ○ Company/Organization

Controller/ Processor roles	Controller (Customer) to Processor (Cillco)
Sensitive data transferred?	None
Frequency of the transfer	Continuous

Nature of the processing	• Providing the products and services, including:
	  ○ Import/export issues and records
	  ○ Track orders
	  ○ Search content
	  ○ Import/export
	  ○ Processing of orders and requisitions
	  ○ Register and view suppliers and contacts
	  ○ Save and store files
	  ○ Display user and company profiles
	  ○ Provide user alerts and messages
	  ○ Request and approve purchase requisitions and orders
	  ○ Forward purchase orders to collaborators

Purpose of the data transfer	• Providing the products and services, including:
	  ○ User and team communication
	  ○ Approvals and permission management
	  ○ File sharing
	  ○ Media management
	  ○ Search
	  ○ Content publishing
	  ○ Communication with collaborators
	  ○ Third-party integration

Duration of processing	Upon termination of service, customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the customer's current subscription period. Cillco retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

Cillco Operations & Analytics (“Usage Data”)	
Categories of data subjects	Customers, customers' employees, customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Cillco Account ID
	  ○ Cillco Cloud ID / Site ID / Tenant ID
	  ○ Segment Anonymous ID
	• Personal Identification, including:
	  ○ IP address
	  ○ Cookie information
	  ○ Device information
	  ○ Browser information
	• Metadata, including:
	  ○ Event Name (i.e. what action the user performed)
	  ○ Event Timestamp
	  ○ Page URL
	  ○ Referring URL

Controller/ Processor roles	Controller (Customer) to Processor (Cillco)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Storing records of user actions performed within products and websites, including support sites and marketing sites
Purpose of the data transfer	Providing the products and services, including: • To provide and administer the products, support, and services, including to calculate usage-based billing • To facilitate security, fraud prevention, performance monitoring, business continuity, and disaster recovery • To comply with legal and financial reporting obligations • To derive insights in order to develop and improve the products, support, and services • To derive insights in order to support business development
Duration of processing	Pseudonymized records of user actions performed within products and websites are retained for 2.5 years in an online and readily accessible format. Aggregated and anonymized records of some key user actions performed within products and websites are retained permanently.

Cillco Support	
Categories of data subjects	Customers, customers' employees, customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Cillco account ID
	  ○ About me
	  ○ Address
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	  ○ SEN (Support Entitlement Number)
	• Personal Identification, including:
	  ○ IP Address
	  ○ Device Information – Mobile
	  ○ Language setting
	  ○ Location/region/city
	  ○ Phone/fax number
	  ○ Screen name/ Handle/ Nickname
	• Employment Information, including:
	  ○ Company/organization

	○ Job title ○ Office location and department association ○ Contact Information ○ Education & Skills ○ Financial Information Personal data in User Generated Content
Controller/ Processor roles	• Controller (Customer) to Processor (Cillco) • Controller (Customer) to Controller (Cillco)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Engage and respond to customer support questions • Marketing activities • Sales activities • Authentication/ System admin • Financial, training and certification • Collect/Manage sales • Analyze business metadata
Purpose of the data transfer	Providing the products and services, including: • Support/ Feedback • Marketing/ Engagement • Account/ Login Management • Business Analytics • Search
Duration of processing	Production customer data is replicated only to a single staging (pre-production) environment. This staging environment is refreshed every 30 days. Support cases are maintained for 5 years after closure. Files attached to support cases are deleted 60 days after case closure.

Appendix B - Security Measures

Description of the technical and organizational measures implemented by the processor(s) / data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymization and encryption of personal data	**Encryption of data** Any customer data in Cillco Applications is encrypted in transit over public networks using TLS 1.2+ to protect it from unauthorized disclosure or modification. Our implementation of TLS enforces the use of strong ciphers and key-lengths were supported by the browser. All persisted data, including personal data, is encrypted using robust AES-256 algorithm in full compliance with GDPR regulations. **Key management** Cillco uses SSE-KMS/SSE-S3 for key management. See https://docs.aws.amazon.com/kms for more information.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Controlling access to customer data** Customer data is handled as sensitive data, and we strive to implement strict controls for governing this data. Awareness is distributed through channels such as the Cillco security board to the rest of the company on best practices for handling customer data. Cillco only allows authorized employees to have access to customer data stored within our platform, through strong authentication mechanisms and access controls such as using individual protected keys for each employee, firewall restrictions, Zero Trust VPN, and two factor authentication secured with Azure Identity protection. If unauthorized or inappropriate access to customer data is detected, it will be treated as a security incident and processed through security management, which includes notifying the customers if a breach of policy is confirmed. **Service availability** Service availability is monitored 24/7 by monitoring mechanisms offered through AWS, complemented by internal monitoring tooling in the Cillco production stack. Detected downtime and issues are without undue delay reported here; https://cillco.statuspage.io **Backup** There is a comprehensive backup routine at Cillco. Using cloud backup mechanisms offered through AWS, files, databases and storage is frequently copied and stored with location resilience for datacenter fault tolerance. Backup is, unless otherwise agreed, kept for 30 days with point in time recovery. **Tenant separation** Customers using Cillco products share a common IT infrastructure, with measures in place to ensure logical separation of data between customers, governed by a Cillco managed identity provider (IDP) in AWS.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	**Business continuity and disaster recovery management** We acknowledge that disruptions happen, so we are determined to plan for disruptions, and handle disruption with minimal impact on our customers when they do occur.

	We utilize redundancy capabilities, such as availability zones and regions, offered by our cloud service providers. We rely on the resiliency of the AWS Cloud Platform and AWS Backup Services. Our disaster recovery tests cover process and technology aspects, including relevant process documentation. The frequency of disaster recovery tests is done in line with the criticality tier of each service – for example, backup and recovery processes for key customer facing systems are tested annually.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	We also perform internal operational audits in areas that are deemed high risk, including a variety of security topics. The results of these audits are reported to the Audit Committee of our Board of Directors and are fed into a continuous improvement cycle that helps us keep sharpening the overall security program.
Measures for the protection of data during storage	**Data centers** Cillco Applications and data are hosted by the industry-leading cloud hosting provider Amazon Web Services (AWS). We use datacenters in EU with the primary region being Stockholm. Redundancy is managed at regional level and across its availability zones. Information on physical security to datacenters can be found; https://aws.amazon.com/compliance/data-center/perimeter-layer **Key management** Cillco uses SSE-KMS/SSE-S3 for key management. See https://docs.aws.amazon.com/kms for more information.
Measures for ensuring physical security of locations at which personal data are processed	Cillco utilizes AWS as preferred cloud provider where Cillco applications are installed and operated. AWS datacenters strictly control physical access to areas where data is stored, and continuously invest in “state of the art” physical security. **Employee Data Center Access** • Access granted only to approved AWS employees. • Employees must apply for access with valid business justification. • Requests follow the principle of least privilege, specifying required data center layers and access duration. • Requests reviewed and approved by authorized personnel. • Access is time-bound and revoked upon expiration. • Granted individuals are restricted to specified areas based on their permissions. **Third-Party Data Center Access** • Third-party access must be requested by approved AWS employees. • Requests require valid business justification and specify required data center layers and access duration. • Access requests follow the principle of least privilege. • Authorized personnel review and approve requests, and access is revoked after expiration. • Visitors must present identification, are signed in, and escorted by authorized staff. • Access is limited to areas specified in the permits. More information here; https://aws.amazon.com/compliance/data-center/controls

Measures for remote/home working	Cillco's security policy only allows company-managed devices to access the Cillco office and cloud infrastructure. Connection is secured by Azure AD authentication with MFA and Conditional Access, complemented by AWS IAM for managing access to cloud resources, and further protected using Zero Trust VPN.