Compliance & Data Protection Policy

Table of Contents

1 Why this policy exists

This data protection policy ensures:

- Complies with General Data Protection Regulation (GDPR) and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

HiveCPQ implements an Information Security Management System in accordance with ISO 27001:2018 in order to meet the requirements. HiveCPQ is ISO 27001 certified and is audited yearly to maintain certificate validity.

2 Data protection law

The General Data Protection Regulation (GDPR) describes how organizations — including HiveCPQ — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

3 Policy scope

This policy applies to:

- The head office of
- All branches of
- All staff and volunteers of
- All contractors, suppliers and other people working on behalf of

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals

- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

4 Data protection risks

This policy helps to protect from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

5 Privacy & Data Protection

HiveCPQ has developed policies and practices, uses security certificates, and communicates best practices with employees and customers. Each HiveCPQ employee is required to take a Security and Privacy Awareness Training and is required to sign an NDA with regard to any Customer Data.

HiveCPQ has put in place a set of technical and organisational measures to comply with GDPR (General Data Protection Regulation of the EU). HiveCPQ acts as a Processor for its Customers (Controller), or as a sub-processor for its SaaS partner (Processor) as defined in the relevant agreement.

Hive CPQ is committed to meet all legal and contractual obligations, in particular those stipulated by the GDPR and the supplemental measures that are to be taken in light of the Schrems II court case of 2020. Our objective is to comply with GDPR and follow good practice in order to protect the rights of staff, customers and partners (all data subjects), to be open about how we store and process individuals' data and to protect ourselves from the risks of a data breach.

<u>General GDPR measures</u> :

- Clear responsibilities outlined for employees, contractors, management and security officer.
- Clear internal data protection policy.
- Technical and organisational measures in place and integrated with our ISMS (audited yearly).
- Awareness & training plan for our employees.
- Data processing registries.
- Support for Data Subject requests to exercise their rights (as relayed by the data controller).
- Data breach notification procedures in place with customers.

Schrems II supplemental measures :

- Clear mapping of data transfers and processing activities outside of EEA.
- Updated Standard Contractual Clauses in place.
- Updated Data Processing Agreements for our customers.
- Continuous monitoring of the legal context and new developments.

5.1 Employee Privacy & Data Protection Training

Every employee of HiveCPQ is required to take the Privacy Awareness and Data Protection Training upon hire, and this training is renewed annually. The core principles are:

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **HiveCPQ will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords and multi factor authentication must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorized people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

5.2 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the CTO.

When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.

- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

5.3 Data use

Personal data is of no value to HiveCPQ unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The CTO can explain how to send data to authorized external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

5.4 Data accuracy

The law requires HiveCPQ to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort HiveCPQ should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Tools & systems will make it **easy for data subjects to update the information** HiveCPQ holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are kept up-to-date** and that **retention policies are enforced**.

5.5 Data Protection Officer

The following is a list of Data Protection Officers at HiveCPQ:

Data Protection Officers		
Frederik Taleman	frederik@hivecpq.com	CEO

Records of Processing Activity

In accordance with article 30 (2) of the GDPR regulation, HiveCPQ's record of Processing activities includes:

- Our contact details, together with those of the Data Controller on whose behalf we are acting and, where applicable, of the Processor's representative and the Data Protection Officer.
- The categories of processing carried out on behalf of the Data Controllers.
- Where applicable, any transfers of the Data to a third-party country together with documentation showing the existence of appropriate guarantees for each transfer.
- A general description of Technical and Organisational security Measures.

Other GDPR Measures

- HiveCPQ only acts on the controller's documented instructions
- HiveCPQ implements measures to assist the controller in complying with the rights of data subjects

- HiveCPQ either returns or destroys the personal data at the termination of a customer agreement.
- HiveCPQ provides the controller with all information necessary to demonstrate compliance with the GDPR

5.6 Other Privacy Standards

HiveCPQ is a Privacy By Design company and takes its users' and customers' data extremely serious. The entire team is continuously involved in data privacy and security and will work with Customers should more stringent requirements arise in the future.

5.7 Data Breach Policy

HiveCPQ has a formal Data Breach Policy in case of data breach of a customer's configuration data in HiveCPQ systems.

Data Breach Policy Summary	
Notifiction to Controller	• HiveCPQ notifies data controller (customer) without undue delay • In case HiveCPQ is the sub-processor, it notifies the processor • Among other measures HiveCPQ may reset passwords, remove HiveCPQ oAuth app
Documentation of Data Breach	HiveCPQ adds the data breach to a GDPR Data breach incident log

6 Data Processing Facilities

Hive CPQ infrastructure (data storages and compute instances) are hosted with Amazon Web Services, which is ISO 27001 certified. AWS implements the following security measures:

6.1 DATA CENTER ACCESS

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

6.2 DATA CENTER ACCESS REVIEW

Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

6.3 REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

6.4 AVAILABILITY

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

6.5 BUSINESS CONTINUITY PLAN

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

6.6 ASSET MANAGEMENT

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

6.7 MEDIA DESTRUCTION

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

6.8 POWER

Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

6.9 CLIMATE AND TEMPERATURE

AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

6.10 FIRE DETECTION AND SUPPRESSION

AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

6.11 CONNECTIVITY

The Hive CPQ service runs in AWS VPCs through private and protected networks. Network security is achieved through VLAN segregation, Firewall policies and internal monitoring. All Hive CPQ infrastructure runs on segregated networks. Internet connectivity is realized by AWS cloudfront.

6.12 MONITORING

Hive CPQ monitors its own servers and services 24/7 and will intervene with first line support in case of infrastructure problems. Second-line escalation to AWS is possible if needed. All SLA and procedures are documented.

6.13 BACKUPS

Hive CPQ implements a backup policy for all servers and files, so that data can be restored quickly in case of human error or equipment fault. Backups are taken every night (RPO is 24h) and each version is kept for 30 days.