Data Privacy Policy

Preamble

When our Customers make use of the Secure Services Hub, they trust us with various types of personal and commercial data and other sensitive information. We understand that this is a big responsibility and work hard to protect the integrity of all data entrusted to us. This Data Privacy Policy shall help our Customers understand what types of data we process in connection with their use of the Secure Service Hub, why we process it, and what rights they have in connection with the processing of their data.

Table of Contents

I. Definitions 2
II. General Information on Processing of Customer Data 4
1. Scope of Data Processing 4
2. Storage Location for Customer Data 5
3. Access to Customer Data 5
4. Processing of Machine Data 5
5. Processing of Personal Data 5
5.1 Overview and Responsibilities 5
5.2 Personal Data Processing as Data Controller 6
5.3 Personal Data Processing as Data Processor 6
III. Individual Data Processing Activities 7
1. Overview 7
2. Processing Activities as Data Controller 7
2.1 Onboarding of Customer Administrator 7
2.2 Provision of Access to Customer Tenant 8
3. Processing Activities as Data Processor 9
3.1 Onboarding of Users 9
3.2 Use of Platform Services 9
3.2.1 Connected and Unconnected Services 9
3.2.2 Service Case Management (Unconnected Service) 10
3.2.3 Machine Documentation (Unconnected Service) 10
3.2.4 Conferencing (Unconnected Service) 11
3.2.5 Remote Access (Connected Service) 12
3.3 Edge Device and Applications 12
3.3.1 Edge Device Activation 12
3.3.2 Maintenance of Edge Devices 13
3.3.3 Application Module Handling 13
3.3.4 Processing of Machine Data by Application Modules 14
3.3.5 Responsibilities for Third-Party Applications 14
IV. Customer Data Security 15
1. Security Architecture 15
2. Important Security Notice 15
V. Amendments of Data Privacy Policy 15

I. Definitions

For the purposes of this Data Privacy Policy, all capitalized terms that are used herein shall have the meanings set forth below, unless context dictates otherwise:

- “**Account**” means an identity created for a named individual that provides access to the Customer Tenant.
- “**Agreement**” means the SaaS Agreement for the Secure Services Hub which describes the services that are provided on the Platform.
- “**Applications**” means the software applications that are made available on the Platform by us and other Application Providers.
- “**Application Backend**” means the service and data storage layer that includes the application programming interfaces (API) of the respective Application.
- “**Application Connection**” means the connection between the Application Module and the corresponding Application Backend that is established when the Application is installed on the Edge Device.
- “**Application Module**” means the Application specific software which is provided via the Platform and runs in the Edge Environment as an encapsulated software container.
- “**Application Provider**” means any service provider who distributes and provides access to Applications over the Platform and is responsible for running the Application Backend of the respective Application.
- “**Application Subscription Terms**” means the contractual terms regarding the use of a particular Application as defined by the Application Provider.
- "**Cloud Service Provider**" means Microsoft Ireland Operations, Ltd., having its registered office at One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18, P521 Ireland, which is engaged to store the Customer Data securely and make it accessible to the Customer.
- “**Connected Services**” shall have the meaning set forth in Section III.4.1.
- “**Customer**” means any legal entity that has entered into the Agreement in order to make use of the Platform.
- “**Customer Administrator**” means the designated named individual who has the permission to administrate the Customer Tenant on behalf of the Customer.
- “**Customer Administrator Account**” means the Account generated by us that enables the Customer Administrator to access and administrate the Customer Tenant.

- "**Customer Data**" means the Personal Data and Machine Data of the Customer that is uploaded to or stored on the Platform by the Customer, transmitted to the Platform Backend or an Application Backend at the instigation of the Customer, or generated by the Platform as a result of the use of the Services by the Customer.

- “**Customer Tenant**” means the Tenant of the Customer that is created when the Customer is onboarded to the Platform.

- “**Data Controller**” means the natural or legal person which determines the purposes and means of the processing of Personal Data.

- “**Data Processor**” means a natural or legal person which processes Personal Data on behalf of the Data Controller.

- “**Edge Connection**” means the connection between the Edge Device and the Platform Backend established when the Machine Asset is connected to the Internet. Technically, the Edge Connection consists of multiple connections that enable the Edge Device to communicate with the services of the Platform Backend.

- “**Edge Device**” means a piece of hardware attached to the Machine Assets that contains the Edge Runtime Environment and that provides the connectivity to the Platform, the Application Backends and the internal network to which the Machine Asset is connected.

- “**Edge Runtime Environment**” means the runtime environment that enables the Edge Device to receive and run Application Modules and communicate the results to the Platform and/or the Application Backend.

- “**GDPR**” means the General Data Protection Regulation (EU) 2016/679.

- “**Hosting Servers**” means the servers operated by the Cloud Service Provider on which the Customer Data is stored.

- “**Identity Management System**” means the identity and access management system used by the Platform to authenticate users and authorize access according to a user's role and permissions.

- “**Machine Assets**” means the machine tools and appliances that can be registered and assigned to a Manufacturer and an Operator on the Platform.

- “**Machine Components**” means the internal components of a Machine Asset that have communication capabilities and can act as data sources or sinks for data that is transmitted to and from an Application Module via the Machine Connection.

- “**Machine Connection**” means a connection between a Machine Component and an Application Module that is installed for the same Machine Asset.

- “**Machine Data**” means any Customer Data that is stored on the individual Machine Components and accessible via established Machine Connections.
- “**Manufacturer**” means a manufacturer of Machine Assets that uses the Platform to provide services to Operators.
- “**Operator**” means an operator of Machine Assets that uses the Platform to make use of the Platform Services and the services provided by the Manufacturers.
- "**Personal Data**" means any information relating to an identified or identifiable natural person.
- “**Platform**” means the cloud-based service portal named Secure Services Hub that facilitates the interaction between Manufacturers and Operators.
- “**Platform Backend**” means the services and data storage layer of the Platform that is hosted on the Hosting Servers.
- “**Platform Portal**” means the front-end presentation layer of the Platform that offers access to the Customer Tenant and acts as the single access point through which specific Application Frontends are accessed by the Participants
- “**Platform Services**” means the services that we provide on the Platform, including the Connected Services and the Unconnected Services.
- “**Service Provider**” means a third-party service provider that uses the Platform to provide services to Operators.
- "**Tenant**" means the dedicated part of the Platform provided for a particular Participant that contains all accounts, assets and data of the Participant and cannot be accessed by any other Participant.
- “**Unconnected Services**” shall have the meaning set forth in Section III.4.1.
- “**User**” means a named individual who has the right to access the Customer Tenant.
- “**User Account**” means any Account created by the Customer Administrator that enables a named User to access the Customer Tenant.

II. General Information on Processing of Customer Data

1. Scope of Data Processing

We only process Customer Data to the extent necessary to provide a functional Platform and to enable our Customers and their authorized Users to make use of our services. Our responsibilities with regard to the individual data processing activities depend primarily on whether the Customer Data qualifies as Personal Data or Machine Data.

2. Storage Location for Customer Data

The Platform is made available via a web-application that can be accessed via the Internet and is hosted on the Hosting Servers operated by the Cloud Service Provider. The Hosting Servers are located in a datacenter located in the European Union. We do not store any Customer Data on our own premises. This means that all Customer Data shared with us as described herein will be transmitted directly from the Customer to the Hosting Servers.

The Cloud Service Provider engages various sub-processors which are located around the world. A complete list of all sub-processors that are retained by the Cloud Service Provider is available under: https://www.microsoft.com/en-us/trust-center/privacy/data-access. To the extent that these sub-processors are permitted by the Cloud Service Provider to access and process Customer Data, this permission is limited to the delivery of services which the Cloud Service Provider has retained the sub-processors to provide.

3. Access to Customer Data

The Platform is designed as a software-as-a-service (SaaS) solution that uses resources of the Cloud Service Provider. Since the Platform is built on a multi-tenant architecture, we create and offer a dedicated Tenant for each Customer. The individual Customer Tenants are logically separated from one another. The Customer Data and other resources of the Customers are fully segregated at all times. For this reason, the Customers can only see and access the data and resources stored within their own Customer Tenant.

4. Processing of Machine Data

While the processing of Machine Data is not subject to the general provisions and principles set forth in the GDPR and other privacy laws, we are aware that Machine Data is of great strategic and economic importance for our Customers. We are therefore committed to full transparency in this regard and strive to illustrate all processing activities and correlated data flows in a clear and comprehensible manner.

As described in Section III.3.3 below, Machine Data can only be accessed and processed by the Application Modules that are made available by the Application Providers and installed on the Machine Assets by the Customer. To install an Application Module, the Customer must accept the corresponding Application Subscription Agreement which sets out the Machine Data processing activities of the Application Module in detail. Machine Data is therefore only collected and processed with the Customer’s consent.

5. Processing of Personal Data

5.1 Overview and Responsibilities

Some of the Customer Data that we process as described herein qualifies as Personal Data. When we process Personal Data in connection with the provision of the Platform, we strive to ensure compliance with the GDPR. Our responsibilities toward the Customer and the individual data subjects primarily depend on whether we process the Personal Data on our own initiative (as the Data Controller) or on behalf of the Customer (as a Processor).

5.2 Personal Data Processing as Data Controller

With regard to Personal Data that is collected and processed by us as described in Section III.2. below, we qualify as the Data Controller. This means that we are fully responsible for determining the purposes and means of processing this Persona Data and do not act on behalf of the Customer or any third party. Enquiries regarding the processing of this Personal Data can be sent to the following address:

Symmedia GmbH, Turnerstraße 27, 33602 Bielefeld, Germany

Our data protection officer (DPO) can be directly contacted at: […]

Whenever we process Personal Data as the Data Controller, the Customer and the data subjects to whom the Personal Data relates can assert the following rights against us as further defined in Chapters 3 and 8 GDPR:

- Right of access by the data subject in accordance with Art. 15 GDPR
- Right to rectification in accordance with Art. 16 GDPR
- Right to erasure in accordance with Art. 17 GDPR
- Right to restriction of processing in accordance with Art. 18 GDPR
- Right to data portability according to Art. 20 GDPR
- Right to object in accordance with Art. 21 GDPR
- Right to lodge a complaint in accordance with Art. 77 GDPR

5.3 Personal Data Processing as Data Processor

With regard to Personal Data that is collected and processed by us as described in Section III.3. below, we qualify as a Data Processor who processes Personal Data on behalf of the Customer. This means that the Customer is fully responsible for determining the purposes and means of processing and must ensure that the processing of Personal Data, including its collection and transfer to us, is based on a lawful basis. To comply with this obligation, the Customer must provide all necessary notices to and obtain all necessary consents from all data subjects (including its employees) to whom such Personal Data relates.

If the processing of this Personal Data falls within the scope of the GDPR, the Customer may be required to conclude a data processing agreement with us. Our **Data Processing Agreement** can be concluded in electronic or physical form.

III. Individual Data Processing Activities

1. Overview

In this Section, we will provide our Customers with detailed information about how we process their Customer Data. To deliver a complete picture, we will illustrate for each processing activity what types of Customer Data we process, for what purpose the Customer Data is processed, for how long the Customer Data will be stored on the Hosting Servers, to whom the Customer Data will be transferred, and, if the Customer Data qualifies as Personal Data, on what legal basis the Customer Data is processed.

2. Processing Activities as Data Controller

2.1 Onboarding of Customer Administrator

The Customer onboarding process includes the creation of the Customer Tenant and the creation of an initial Customer Administrator Account with administrator rights for the Customer Tenant. A successful Customer onboarding process ends in the status that the Customer Tenant is created and the initial Customer Administrator has received an email to activate the Customer Administrator Account (see **Onboarding of Users**).

The Customer onboarding process can either be initiated by us, by the Customer, or by a Service Provider. In all these cases, we collect and process the following information related to the Customer Administrator ("**Administrator Data**"):

- Name and address of the Customer
- Email address of the Customer Administrator
- Bank data for the purpose of automated billing (if applicable)

We collect and process the Administrator Data to identify the Customer Administrator as the unique owner of the Customer Administrator Account and ensure correct and secure billing. By collecting and processing the Administrator Data, we can prevent possible inconsistencies in the Customer onboarding process and ensure that the invitation to access the Customer Tenant will only be sent to the email address of the individual who is designated as the Customer Administrator by the Customer

The Administrator Data will be stored on the Hosting Servers in encrypted form until the Agreement is terminated. In case of a termination of the Agreement, we reserve our right to retain the Administrator Data for an additional ten (10) years before it is deleted from the Hosting Servers and redacted from the Agreement. This additional storage of the Administrator Data is required to ensure that we can meet our obligations under potentially applicable data retention laws.

Since the processing of the Administrator Data as described is necessary to perform our contractual obligations under the Agreement, the processing is based on art. 6(1)(b) GDPR. We will not disclose to or share the Administrator Data with any third party other than the Cloud Service Provider without the Customer’s specific, informed and unambiguous consent within the meaning of art. 6(1)(a) GDPR, unless a disclosure is necessary to comply with a legal obligation to which we are subject as set forth in art. 6(1)(c) GDPR.

2.2 Provision of Access to Customer Tenant

As described in the Agreement, we make use of the enterprise identity service Azure Active Directory to provide access to the Platform. The Users are therefore able to log in to the Customer Tenant using the existing credentials which are provided by the Identity Management System of the Customer. From a technical perspective, we invite the existing profile of the User to our Platform directory. This means that we are not required to generate or hold any usernames or passwords for the Customer Administrator and individual Users.

When a User accesses the Customer Tenant for the first time, the User will be asked for his or her consent to share the following information with us, which is already stored in the Identity Management System of the Customer (“**Identity Management Information**”):

- Name of the User
- Email address of User
- Photo of the User (if applicable)

We process the Identity Management Information in order to authenticate the User during the login process, associate specific access permissions with the User’s identity, and sign the User in to the respective account. The Identity Management Information is further used to enable 'single sign-on' for the User, which allows the User to use his existing credentials provided by the Identity Management System.

The Identity Management Information will be stored on the Hosting Server until the respective account is deleted or until the User withdraws his or her consent as described below. Once the User withdraws his or her consent or the respective account is deleted, we reserve our right to retain the Identity Management Information for an additional ten (10) years before it is deleted from the Hosting Server. This additional storage of the Identity Management Information is required to ensure that we can meet our obligations under potentially applicable data retention laws.

Since we only process the Identity Management Information based on the explicit consent of the User, the processing is based on art. 6(1)(a) GDPR. The User can withdraw his or her consent at any time by visiting […]. We will not disclose to or share the Identity Management Information Data with any third party other than the Cloud Service Provider without the specific, informed and unambiguous consent of the User within the meaning of art. 6(1)(a) GDPR, unless a disclosure is necessary to comply with a legal obligation to which we are subject as set forth in art. 6(1)(c) GDPR.

3. Processing Activities as Data Processor

3.1 Onboarding of Users

Once the Customer Administrator Account is activated, the Customer Administrator will be able to invite additional Users to the Customer Tenant and administrate their access rights and permissions. The Customer Administrator can create any number of User Accounts and determine which authorization each User should have. When creating a new User Account, the Customer Administrator requires the email address of the respective User in order to trigger the onboarding process.

The onboarding process can be initiated for Users who already have an account linked to Microsoft (e.g., due to a business account based on Azure Active Directory) and Users who do not have an account linked to Microsoft (e.g., private individuals or employees of Customers that do not use Azure Active Directory or similar service). Apart from the differences described below, the onboarding process will look the same for both types of Users.

Once the User onboarding process is initiated, the invited User will receive an automatically generated email from Microsoft which contains information about the organization that initiated the invitation as well as the domain and system to which the User is invited. An example of such a mail looks like this: […].

[…]

The final step in the onboarding process is the User’s confirmation and acceptance of this Privacy Policy and the creation or linking of their User Account to the Customer Tenant. Once the Privacy Policy is accepted, the User is redirected directly to the Platform Portal. Depending on the internal security policies of the Customer, additional authentication mechanisms like 2-Factor-Authentication may be triggered.

3.2 Use of Platform Services

3.2.1 Connected and Unconnected Services

Our data processing activities related to the use of the Platform depend on the Platform Services that are used by the Customer. Platform Services are related to Machine Assets that are registered in the Customer Tenant. The availability of Platform Services further depends on the compatibility of their Machine Assets. Not all Services are available for all Machine Assets. The Platform Services are divided into the following categories:

- The services in the first category (“**Unconnected Services**”) are offered to all Customers and do not require a real connection between the registered Machine Asset and the Platform. The Unconnected Services for example include the Services Service Case Management with Video and Voice Communication.

- The services in the second category (“**Connected Services**”) can only be provided if the corresponding Machine Asset is equipped with an Edge Device that connects the registered Machine Asset to the Platform. All Connected Services are separate Applications that must be installed on the Edge Device as described herein.

Any Personal Data that is processed as part of the provision of the Platform Services can only be linked via references to technical universally unique identifiers (“**UUIDs**”) across the Platform. If a User Account is deleted, the reference becomes invalid, and it can never be traced back to the corresponding User. We will not disclose to or share any Customer Data related to the use of Platform Services with any third party other than the Cloud Service Provider without the specific, informed and unambiguous consent of the User, unless a disclosure is necessary to comply with a legal obligation to which we are subject.

3.2.2 Service Case Management (Unconnected Service)

Service Case Management allows Operators to send service requests to the Manufacturers or Operators concerning a particular Machine Assets (“**Service Requests**”). By creating a Service Requests, Operators can for example order a spare part, report a problem, or sign up for an upcoming inspection. The Service Requests can be used to provide critical information to the recipient, including the following (“**Service Data**”):

- A detailed problem description
- Prioritization of the request according to urgency, service level, etc.
- Possibility of direct connection to the Machine Asset (see **Remote Access**)
- Escalation Process
- Documentation
- Automatic forwarding outside business hours (daylight following)

The Service Data is collected via the corresponding forms of the Service Request ticket. Depending on the configuration, the required and optional fields vary. Due to the fact that Service Requests are always linked to a Machine Asset, important information about the Machine Asset such as log files or Machine Asset ID can be automatically attached to the Service Request. The responsibility for information that is manually entered in the context of a Service Request lies with the Operator or Service Provider.

3.2.3 Machine Documentation (Unconnected Service)

Machine Documentation allows all Customers to manage documents of any kind such as the maintenance manual of a Machine Asset from the Manufacturer or specific adjustments that were made to a Machine Asset by the Operator. The purpose of Machine Documentation depends on the role of the Customer:

- For Manufacturers and Service Providers, the purpose of Machine Documentation is that they can store corresponding documents for each supported Machine Asset or machine type. These documents can then be viewed by all Operators who are using the corresponding Machine Asset or machine type.
- For Operators, the purpose of Machine Documentation is that they can store individualized documents related to particular Machine Asset that is registered in the Customer Tenant. These documents can then be used by Users who have access to the Customer Tenant.

In both cases, only the User who has uploaded the respective document has the possibility to remove or change the document. This User is also responsible for the contents of the documents without exception as well as the compliance with legal regulations and laws and applicable data protection regulations.

3.2.4 Conferencing (Unconnected Service)

Conferencing includes various possibilities of collaboration between participants on the Platform, which can either be used integrated in other Platform Services such as Service Case Management, but also detached from them. Conferencing enables Users to communicate with other Users within the same Customer Tenant or with Machine Manufacturers and Service Providers on other Tenants.

Chat Function

Users can use the Chat Function to communicate directly and quickly via text messages over the Platform. This includes both group chats with Users within the same Customer Tenant as well as chats with Manufacturers and Service Providers beyond the boundaries of the Customer Tenant. Besides text messages, Users can also attach files or whiteboards to a chat. The text messages, files and whiteboards that are created or uploaded by the Users can only be accessed by the participants of that chat.

The Chat Function is implemented with the open source framework Matrix (see http://Matrix.org). […] The runtime instance is operated by the external service provider Ungleich.ch (see: https://ungleich.ch/) and integrated into the Platform. All data that is submitted by the Users in connection with the use of the Chat Function is stored on the Hosting Servers and remains there until both participating Tenants no longer exist.

The Users who are writing text messages and uploading files and whiteboards are responsible for such content without exception as well as the compliance with legal regulations and laws and applicable data protection regulations.

Video Conferencing

Users can use Video Conferencing to communicate with each other directly and via video. With regarding to visibility, participants, and storage of data, Video Conferencing is subject to the same rules as the Chat Function. The transmission of video streams is encrypted by the Platform. The video streams are always temporary and never stored on the Hosting Servers. The oral and visual information that is shared during a video conference can therefore not be traced or accessed in retrospect.

3.2.5 Remote Access (Connected Service)

Remote Access provides a complete remote maintenance infrastructure and thus forms the basis for efficient troubleshooting in the event of a malfunction of a Machine Asset. It allows Manufacturers and Service Providers to access the Edge Device of a compatible Machine Asset and is therefore very closely linked to Service Case Management, which in many cases precedes Remote Access. In order to protect the integrity of the Machine Assets, Remote Access can only be requested and activated by the Operator.

Remote Access takes place via a highly secure connection. In addition to desktop sharing or file transfer, services for accessing controllers (such as Siemens S7, Beckhoff, etc.) are available to the Manufacturer or Service Provider. With the appropriate authorization, the controller software can be accessed and even changes to the programming can be made. The scope of access granted to Manufacturers and Service Providers as part of Remote Access can be defined by the Operator on an individual or general basis. Every access and every function that is executed as part of Remote Access is tracked by the system and can be viewed by the Manufacturer and the Operator until the Edge Device is removed.

The data that is exchanged during a Remote Access session is the full responsibility of the participating parties. The Platform only establishes a secure and encrypted connection and therefore cannot and does not read or store any data.

3.3 Edge Device and Applications

3.3.1 Edge Device Activation

In order to use Connected Services such as Remote Access which are made available via Applications on the Edge Device, the Customer must establish a connection between the Edge Device and the Platform by connecting the Edge Device to the Internet via Ethernet cable ("**Edge Connection**"). The Customer can disable the Edge Connection at any time by disconnecting the Machine Asset from the Internet.

Once the Edge Connection is established, the initial boot process can be started. When the Edge Device is started for the first time, it uses the Internet connection to establish a connection to the platform backend based on the preset configuration. This connection is protected via HTTPS. The Edge Device is delivered with a certificate for this purpose, which is installed during the provisioning process. During this handshake, only the unique Edge Device ID is transmitted to the platform backend. Based on this ID, the platform backend can establish a unique association with the Customer and validate the implicitly requested CSR (Certificate Signing Request) and issue a new certificate to the Edge Device for subsequent secure operation. As soon as the process is complete, the Edge Device is registered in the Platform Backend and can be used with corresponding Applications.

3.3.2 Maintenance of Edge Devices

The Edge Connection is a two-way communication channel between the Platform and the Edge Device (see visualization below). Once the Edge Connection is created, we are able to pull and push data from the Edge Device to the Platform Backend and vice versa and execute arbitrary commands on the Edge Device to perform maintenance tasks.

These maintenance tasks allow us to keep the Edge Device and the software installed on the Edge Device operational, update the Edge Runtime Environment as well as basic software components, and support the Customer in case of functionality issues, for example by performing analysis tasks such as checking log files. In order to protect the integrity of the Machine Components and the Customer Data that is stored thereon, we do not pull or push any data from the Machine Components to the Platform Backend and vice versa, unless the Customer decides to download any of the Applications described below.

The Edge Device does not have a permanent connection to the Platform Backend. Any necessary maintenance issues, e.g., if the Edge Device is no longer working correctly or the environment needs to be updated or repaired manually, are handled via a defined and secure process. As part of this process, we connect to the Edge Device via an SSH tunnel with a signed temporary certificate. The counter certificate for validating the request is already available with the provisioning of the Edge Device. The generation of the temporary certificate, as well as the access to the Edge Device itself, are both logged and can therefore be viewed historically. Any Customer Data that is transmitted as part of a maintenance activity or transferred to the Edge Device is used solely for the purpose of maintenance. We will never access or transfer any Customer Data outside of this purpose.

3.3.3 Application Module Handling

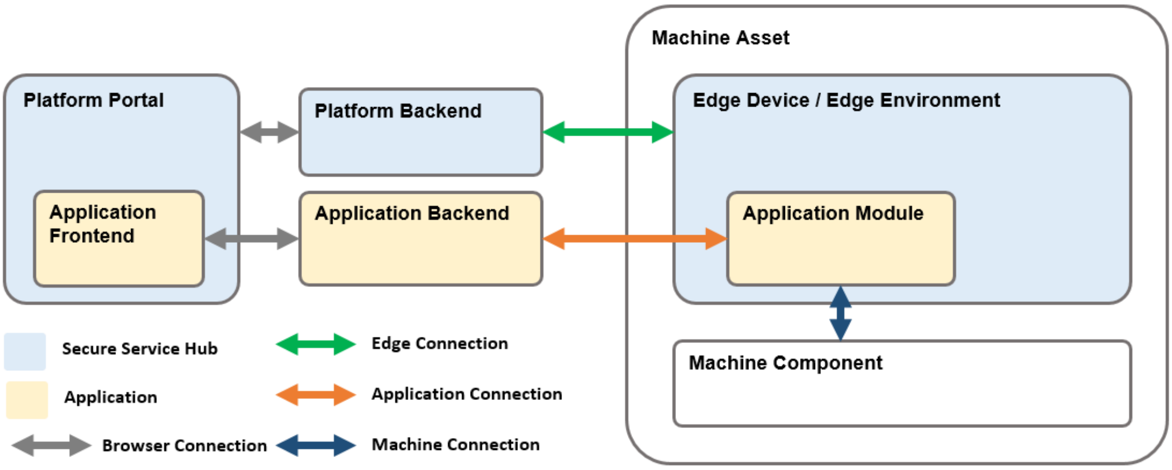
Every Connected Service, whether offered by us of by a third party, is delivered as part of an Application. The functions of these Application and the handling of Customer Data by these Applications must be described separately in each case. For Applications that are made available by us, this information can be found in the "Connected Services" area. Third Party Applications come with a separate Application Subscription Agreement, which must be accepted by the Customer (see **Responsibilities for Third Party Applications**).

Each Application contains an Application Module that must be installed by the Customer on the Edge Device of the selected Machine Asset. Application Modules enable the exchange of data between the Application Backend and Machine Components by simultaneously creating the following two connections (see visualization below):

- The Application Connection is a two-way communication channel that enables the exchange of data between the Application Backend and the Application Module that is installed on the Edge Device.
- The Machine Connections are two-way communication channels that enable the exchange of data between the Application Module on the Edge Device and the individual Machine Components that are required for the Application to function.

3.3.4 Processing of Machine Data by Application Modules

As illustrated in the visualization below, the Machine Data that is stored on the individual Machine Components can only be accessed via Machine Connections. This means that the Customer will only provide access to Machine Data if the Customer Administrator installs Application Modules on the Machine Assets. No other part of the Platform will have access to the Machine Data of the Customer.



The Application Provider is technically able to access all Machine Data that is stored on the Machine Components connected to the Application Module. However, Application Modules only require access certain types of Machine Data in order for the Application to function. Since every Application Module processes different Machine Data, Application Providers are required to prepare separate Application Subscription Terms for their Applications which contain the following minimum information and must be accepted by the Customers:

- List of all Machine Connections that are created by the Application Module;
- List of all Machine Data that is accessed via the Machine Connections, including information on storage, deletion and transfer of such Machine Data; and
- List of all Personal Data that is processed by the Application Provider

Application Providers must further adhere to the principle of data minimization and limit the collection, storage, and usage of Customer Data to data that is relevant, adequate and necessary to ensure the proper functioning of the Application.

3.3.5 Responsibilities for Third-Party Applications

When the Customer installs an Application of a third party Application Provider, we merely act as a facilitating intermediary between such Application Provider and the Customer. This means that the respective Application Provider is responsible for determining the purposes and means of processing the Machine Data and must inform the Customer accordingly. If an Application Module processes any Personal Data, the Application Provider must further ensure that the processing of Personal Data is based on a lawful basis.

To offer an Application on the Platform, third-party Application Providers must contractually agree to limit their data processing activities to the Machine Data and the purposes listed in their Application Subscription Terms. If the Customer suspects or becomes aware that an Application processes any additional Machine Data, we kindly ask the Customer to send us a corresponding note so we can take appropriate measures.

While we are technically able to access all Machine Data that is transferred to Application Modules, we will never pull any data from Application Modules that are not part of our own Applications. This means that we will only process Machine Component Data if the Customer installs an Application that is provided and operated by us.

IV. Customer Data Security

1. Security Architecture

The Platform is built with strong security features that protect the Customer Data. To protect Customer Data from loss and unauthorized access, we have implemented various security measures into our Services which are detailed in our **Security Whitepaper**. In addition to these technical security measures, we restrict access to Personal Data to employees, contractors, and agents who need to have access in order to process the Personal Data. Anyone with access to Personal Data is subject to strict contractual confidentiality obligations and may be disciplined if they fail to meet these obligations.

2. Important Security Notice

The access to the Platform and our Services is provided via a web application. This means that the security and integrity of the Customer Data depends to a large extent on the integrity of the computer systems used to access the Customer Tenant. As specified in the Agreement, we do not accept any liability for the disclosure or manipulation of Customer Data in connection with the manipulation of computer systems.

V. Amendments of Data Privacy Policy

We reserve our right to update this Data Privacy Policy at any time in compliance with the GDPR and other applicable data protection regulations. We will inform about such changes by making an updated Data Privacy Policy available in the Customer Tenant. All changes become applicable as soon as they are made available in the Customer Tenant.

If there are substantial changes to the way we process Customer Data, we will post an additional change notice in the Customer Tenant at least 30 days before the changes become effective. Any use of the Platform and the Platform Services after such changes have become effective will be subject to the updated Data Privacy Policy.

This privacy policy was last updated in […] 2022.