Dataprotection Policy

Introduction

According to our business model which is clearly focused on business to business markets, TTTech does not process personal data of consumers. Nevertheless our business partners expect that we handle the personal data of their employees with care and that we fully comply with all requirements of the European Union's-General Data Protection Regulation (EU-GDPR), the Austrian Federal Act concerning the protection of personal data (DSG) and other applicable country specific legislation, to demonstrate that we are a reliable and trustworthy partner.

Scope

This policy applies to all employees and external partners of all TTTech Companies who process personal data or related personal identifiable information.

Goals

Goal of this policy is to provide the basic definitions on personal data, to define the organizational controls to effectively protect personal data within the TTTech Companies, and to guarantee the rights of the data subjects according to the Articles 12-22 of the EU-GDPR.

Basic-Definitions

The following definitions of terms used in this document are drawn from Article 4 of the EU-GDPR.

- **personal data** means any information relating to an identified or identifiable natural person ('data subject')

- **data subject / identifiable natural person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- **pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

- **controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

- **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

- **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

- **personal data breach** (or **data breach)** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- **genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

- **biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

- **data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

- **special categories of personal data** are particularly sensitive in relation to fundamental rights and freedoms, where disclosure of such data could lead to physical damage, severe financial loss or damage to the reputation

Specific Definitions

The following definitions of terms are derived from definitions in the EU-GDPR but are adapted to specific needs of our data protection procedures.

- **data class:** a classification scheme which contains information of the riskiness of the processing of the associated personal data. i.e it tells the user which impact on the rights and freedoms of a data subject can be expected in case of a data breach
- **categories of data:** a group of data attributes that are related / provide similar information. In the EU-GDPR this is also sometimes referred to as 'type of personal data'
- **type of data subject:** a group of data subjects that are related or share the purpose in our processing activities. In the EU-GDPR this is referred to as 'categories of data subjects'
- **recipient type:** a group of legal entities or organizations that can receive personal data

Types of data subjects

- **Employees:** all staff of TTTech Companies with employment contracts
- **external employees:** all people working for TTTech Companies who are not employees
- **Partner contact:** the staff working for suppliers and other partners who are not external employees
- **Customer contact:** the staff of our customers and prospective customers
- **Consumer:** all other data subjects who are in most cases the buyers of our customers products

Categories of data

The following table contains a list of sample data attributes associated with the data categories and data classes. The list should cover the most relevant processing activities but it can not be considered complete.

Data class	Data category	Data attributes

Basic	Master data	first name, last name, age, sex, nationality, date of birth, place of birth, family status, employee number, employee user-id, customer number
	Address data	country, town, zip-code, street, house number, door number
	Contact data	phone number, mobile number, e-mail, messenger IDs, fax number
High	Identification data	consumer user-id, social security number, tax number, bank account number, password, security questions, ID-Card number, copy of ID-Card, licence plate number, IP-Address
	Usage data	login log, logout log, internet usage, connection times, call connection, position information
	Financial data	salary, bank balance, credit rating, distraint, credit card data, transaction data, debit data
	Presence data	working hours, time recording, work details, absence reasons
	Marketing	income, spending capacity, consumer behavior, details regarding household
Special	Biometric data	face recognition, finger print, DNA, iris scans
	Health data	probes, diagnostic data & findings, allergy, health risks, degree of disability
	Criminal records	criminal offenses, convictions, security measures, CRB check
	Other special data	racial or ethical origin, religious or philosophical belief, trade union membership, sex life or sexual orientation, profiling data, video and audio recordings

Recipient types

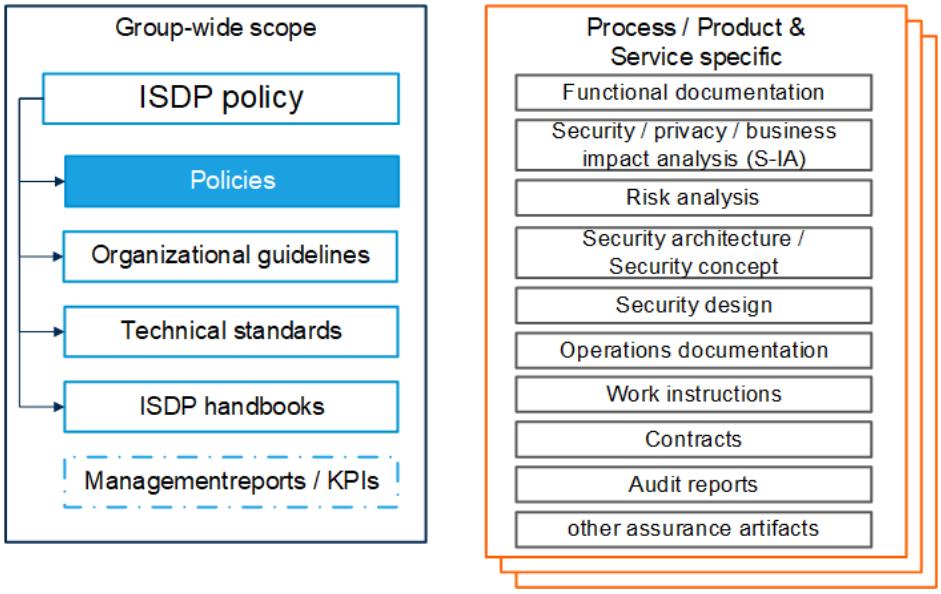
To support the maintenance of the records of processing activities the following recipient types are defined.

- **internal recipients:** this type is to be used for all data processing activities that are conducted within the same legal entity as the source activity
- **group with EU-level:** this type shall be used for all processing activities within TTTech group and on premises within EU-member states or states listed in the EU-Adequacy decisions
- **group outside EU:** this type shall be used for all processing activities within TTTech group

- **partner & customer with EU-level:** this type shall be used if personal data is submitted to business partners or customers that process this data within the EU-member states or states listed in the EU-Adequacy decisions
- **partner & customer outside EU:** this type shall be used if personal data is submitted to business partners or customers that process this data in other countries
- **supplier with EU-level:** for all submissions to suppliers with processing within the EU or states listed in the EU-Adequacy decisions
- **supplier outside EU:** for all submissions to suppliers with processing in other countries
- **authority within EU:** for all submissions to authorities of EU-member states
- **authority outside EU:** for all submissions to authorities of other countries

Document hierarchy

This policy is part of the groupwide Informationsecurity & Dataprotection management system and is located in the document hierarchy as follows



Basic Concepts

Data protection principles

The following principles shall guide our daily work with personal data and personal identifiable information and must be followed by all employees.

- **Lawfulness of processing:** We only process personal data, that we need to fulfill our contracts, to comply with legal regulation, to support our safety engineering efforts of our

products to protect the vital interests of data subjects, or for which we have the documented consent of the data subject. Furthermore, we don't process data of data subjects aged below 16 years.
- **Adhere to purpose:** We only process personal data according to the documented purpose it was collected for.
- **Data minimization:** We only use the minimal necessary set of data attributes we need to fulfill the purpose of our processing activities and we delete personal data we no longer need to fulfill this original purpose.
- **Data security:** We protect the personal data we process from disclosure according to the state of the art, we do not circumvent protection measures and we assure the accuracy and integrity of the personal data. This also means we adhere to the "need to know" security principle
- **Privacy by default:** All our IT-systems used for processing personal data are configured by default to implement data minimization and data security, and in addition our products are configured in that way too at the time they are delivered.

Core roles and responsibilities

The following roles build the backbone of the data protection management system and it's activities.

Employees & Business Partners

All employees no matter if they are internal or external staff and all business partners must adhere to the data protection principles above, and

- report suspected data breaches in the same way as other security incidents according to the requirements stated in the security at the workplace policy as soon as they recognize them
- support the data owners and data protection coordinators in their tasks (especially to ensure the data subject rights)
- attend data protection training
- classify documents containing personal data or PII according to the classification scheme defined in the security at the workplace policy

Data Owner

The data owner is a member of line management who is accountable for a defined set of data. For the purpose of this policy the set must be defined by the data attributes and the types of data subjects. (e.g. a data owner can be responsible for all master data of the employees.) This means the data owner

- defines the processing purpose the data will be used for, and therefore must approve requests to use this data in business processes / business procedures

- is accountable for the security of that data and must ensure that a security concept according to Art. 32 EU-GDPR is defined and enforced for all processing activities the data is used in
- is accountable that the data subject rights can be guaranteed for the data set
- is accountable that the time limits for the storage of this data set are defined and enforced

The data owner role is a management role, that must be assigned at least to group level functions, and can not be delegated further. However, the responsibility for the tasks associated with this role can be assigned to normal employees.
The data owner role should be assigned to those process owners whose processes generate the personal data or that are the primary activity.

Line Management / Process owner

The line Management is accountable for the processing activities that use personal data. This means they take the role as process owner who has

- the accountability for the correctness and completeness of the processing activity record of their process or procedure
- the accountability that the security concept according to Art. 32 EU-GDPR is defined for their process and enforced
- to support the data owner in assuring the data subject rights
- to ensure that all staff working in the business process has data protection training at least once a year

Service Owner

The service owner (see Glossary @ ISDP-Policy), who should be member of the line management, has

- the accountability that the data processing agreements (DPAs) for all subcontractors needed to provide the IT-Service are signed / part of the contract
- to support the process owner / data owner in creating and maintaining their security concept
- to support the data owner to implement the data subject rights

Data Protection Coordinator / Data protection contact

The responsibilities of the data protection coordinator and the data protection contact are specified in the ISDP-Policy.

Information Security Officers

The Information Security Officers (ISOs - see ISDP-Policy) shall support the data owner, process owner and service owner in creating and maintaining the security concept either by coordinating the needed security architects or by taking the security architect role by themselves.

The ISOs shall guide the data-, process-, and service owner through the data security related processes.

the following sections are primary relevant for data owners, process owners, service owners and the data protection coordinator / data protection contacts

Data protection activities

The following activities need to be performed in order to be compliant to the requirements of the EU-GDPR.

Records of processing activities (RPA)

The records of processing activities is, according to the EU-GDPR the documentation of all processing activities (i.e. business processes using personal data). Therefore every business process and business procedure must have a written documentation that contains at least the following information

- The name of the processing activity / business process / procedure and a groupwide unique identifier
- The business unit of the process owner
- The name (given and last name) of the process owner
- The purpose of the processing activity (i.e. what is it good for) / this can also be a reference to a more detailed description of the process / procedure
- The legal basis (i.e. legal requirement / contractual obligation / protection of vital interests / consent) for the processing activity according to art. 6 & 9 EU-GDPR.
- A list of all types of data subjects according to the definitions in section data subject types whose data are processed
- A list of all data types according to the definitions in section data categories that are processed
- A list of all recipients that the data processed will be forwarded to or disclosed for further processing according to the definitions in section recipient types.
- To support the implementation of the data subject rights at least the process / procedure documentation or the documentation of the used IT-Services must contain a description which data-attributes are forwarded / shared with other processing activities including the direction of the data flow.
- The time frame for which the data is needed starting from either the date of collection or the date of contract termination or the end of life in case of a PLC related processing, including the legal / contractual basis
- The information if TTTech acts as controller as joint-controller or as processor for the processing activity
- The information if a data protection impact assessment (i.e. a detailed risk analysis for the processing activity) is necessary, the link to the privacy impact assessment (a raw /

superficial risk analysis for the processing activity) and the link to the security concept according to the Art. 32 EU-GDPR
- The link where eventually needed (in case that some parts of the processing is outsourced) data processing agreements, and the documentation of further safeguards according to Art. 45 & 46 EU-GDPR, related to the processing activity are stored.
- The date of the last review of the RPA, the name of the person who conducted it, and formal approval of the process owner
- The date of the initial (and subsequent in case of major changes in the processing activity) formal approval of the data owner(s) and their names

To support transparency regarding the RPA all RPAs must be stored in a central location or an appropriate data protection management tool.

Information & Access to personal data / data subject rights

According to the Articles 13 to 21 EU-GDPR the data-subject has to be informed at the time of collection about the purpose (and further details listed below), and has the right of access, rectification, erasure, restriction of processing, notification, data portability and the right to object the data processing.

Information at data collection

It is the responsibility of the data owner or one of his / her employees to inform the data subject at the time of collection of his / her data about the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Company's security measures to protect personal data for all intended processing activities. Furthermore the data owner is responsible for providing / maintaining evidence in case the processing is based on the consent of the data subject. The data protection contact and data protection coordinator shall support the data owner in performing this task by providing templates for this data protection notice and by giving guidance on the mandatory contents according to Art. 13 EU-GDPR.

In any case where the personal data is not obtained from the data subject the information of the data subject shall be done according to the definitions above.

Right of access & data portability

It's the responsibility of the data protection coordinator to define a procedure that provides a single interface for data protection inquiries and routes those to the appropriate data owners, as well as the service owners of the services used for data processing, and that routes the appropriate information back to the data subject within 30 days. To support this process adequately it's the responsibility of the service owners to provide / implement a technical interface that allows the timely copy of all personal data of a defined data subject in a secure way.

Rectification & erasure

It's the responsibility of the data protection coordinator to define a procedure that routes inquiries regarding the right of rectification and erasure to the appropriate data owners, process owners and the service owners of the services used for data processing. The process must ensure a timely correction of the data and an information of the data subject regarding the status of his / her request which in case that it can't be fulfilled must contain further information about the reason, or a time frame till when it can be executed successfully. To support this process every IT-Service that processes personal data must support expiry dates for the data objects.

Restriction of processing and objecting

It's the responsibility of the data protection coordinator to define a procedure that routes inquiries regarding restriction of and objection to processing to the data owners, process owners and the process owners, and that informs the data subject about the status of his / her request within 30 days, and in case that it can't be fulfilled the information about the reason, that goes conform to the requirements with Art. 21 EU-GDPR.

Notification of data recipients

It is the responsibility of the data owner or one of his / her employees to notify all recipients of the personal data in his / her area of responsibility on all requests to rectify or erase personal data or the restriction of it. In Addition the data owner shall provide the information needed to inform the data subject about the recipients in case this is requested.

Storage limitation

To support data privacy by design each it-service used to process personal data shall also contain meta information for each data set which defines the expiry date of the information. In addition each it-service used to process personal data shall contain a garbage collection mechanism, that erases personal data automatically according to the expiry date at least once a month. The garbage collection mechanism must also consider backup and archiving mechanisms and must guarantee that the personal data that is no longer needed is also deleted from these systems at least at the end of the calendar year of the expiry date, and that deleted personal data is not restored to live systems after the expiry date.

Data processing agreement

A data processing agreement used as basic agreement regarding the processing of personal data on behalf of TTTech must contain at least the following information

- name, address and commercial register number of the controller
- name, address and commercial register number of the processor and all of his subcontractors
- the obligation for the processor to comply with the EU-GDPR

- the list of data categories and data subject types that are subject of the processing including the information which of these need to be processed by the subcontractors
- the purpose of the processing, i.e. the link to the underpinning contract
- all security measures needed / implemented at the processor (and his subcontractors)
- requirements regarding data protection training for the processor staff
- requirements how the processor has to assist the controller regarding the data subjects rights
- details regarding the right of the controller to conduct data protection audits
- details how the processor has to assist / inform the controller in case of a data breach
- details regarding the return of data to the controller and the secure deletion of data
- information how the processor chooses new subcontractors and details regarding the right of the controller to terminate the processing in this case
- details regarding the submission / transport of personal data outside of the EU
- information about the disclosure of personal data to legal authorities

The data protection coordinator shall provide a template for a data processing agreement that shall be used as standard by all data owners, process owners and service owners.

Data breach handling

In order to comply with the requirements of Art. 33 and 34 EU-GDPR the data protection coordinator must define a procedure that incorporates the following requirements

- data breaches and suspected data breaches must be treated as security incidents
- every stakeholder (i.e. employee, partner or customer) shall have the possibility to report a suspected data breach
- the analysis of the suspected data breach must start within a maximum of 24 hours and a confirmation statement shall be ready within another 24 hours
- in case the data breach is confirmed during the analysis it must be reported to the according supervisory authority within 60 hours after the confirmation
- in case the data breach results in a high risk (according to the privacy impact assessment) for the affected data subjects they have to be informed by electronic means as soon as possible and the notification should include recommended measures for the data subjects to limit the risk.
- in case TTTech acts as processor the affected controller, which in most cases is our customer, must be informed as soon as the breach is confirmed

Security Concept

According to the requirements of Art. 32 EU-DSGVO a security concept for a processing activity must contain at least the following items

- A detailed description, or at least a link to the description, of the processing activity including the most relevant work steps and the it-services used by them
- A privacy impact assessment, and in case of a high risk for the data subjects a detailed risk assessment or data protection impact assessment
- A structural description of the components of the it-services and the technical interfaces used for data transport
- A description of the appropriate organisational and technical security measures needed to contain the risk for the data subjects within social acceptable limits
- A description about the actual state of the implemented security measures including an evaluation of the actual residual risk for the data subjects
- For those processing steps or IT-Services that are completely (BPaaS / SaaS) or partially outsourced (PaaS and IaaS) their security concepts / security documentation must also contain evidences regarding the effectiveness of the implemented measures of the processor / service operator