1 Introduction

Tag Systems Smart Solutions, hereinafter referred to as TSSS, delivers cutting-edge products, services and technologies to the payment, government and industrial sectors. Privacy is a core issue for TSSS and we aim to always secure your personal data. As security and Privacy are at the heart of augmented identity, the secured digital way of identification we propose, TSSS has declared security and Privacy as vital criteria in the pursuit of our mission.

In an increasingly digital world, the boundaries and definition of security are changing. TSSS's security strategy implements the best security standards encompassing both the physical and digital worlds, without forgetting the intertwined interconnections between these worlds.

To achieve our requirements, TSSS is committed to safeguarding our customers' business interests and our own by providing comprehensive cybersecurity and information protection services.

The TSSS personal data strategy is based on Privacy by default and Privacy by design principles.

2 Definitions

For the purposes of this document, the following definitions apply:

Anonymization	The technical method of de-identification of personal data in such a manner that the data can no longer be attributed to a specific Data Subject
Confidential Information	Any information defined as confidential per the Information Classification Policy.
Cookie	A small amount of data generated by a website and saved by your web browser.
Data Controller	The person/entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Protection	All rules and regulations related to personal data protection in the world.
Data Processor	The person or entity which processes personal data on behalf of the Data Controller.
Data Subject	An individual whose personal data is processed manually or automatically.
Data Sharing Agreement	Agreement within Austriacard Group, between two affiliates, enabling personal data transfer with the same level of data protection.
Data transfer	Any data communication, copy, access and/or transmission via network, or from one medium to another, irrespective of the type of medium, outside the European Union (EU), to third countries or international organizations, to the extent that such data are intended for processing by the recipient.
Employee	Any person who is or was in an employment relationship with TSSS, such as apprentices, trainees or temporary workers, former employees, and contractors.
Austriacard Group entities	All companies of which Austriacard Holdings, either directly or indirectly, holds more than half of the registered capital and/or companies which Austriacard Holdings directly or indirectly controls or manages.
TSSS Assets	All tangible and intangible Assets that TSSS has.

personal data	Any information relating to an identified or identifiable natural person (a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, etc.).
personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Privacy	All information and data related to Privacy matters of an individual or of an entity which includes but is not limited to personal data and Confidential Information, trade secrets, or any information related to Privacy in general.
Processing of personal data	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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymization	The processing of personal data in such a manner that the 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 organizational measures to ensure this.
Purpose of processing	The reason for the personal data processing.

Personal Sensitive data	Personal data is considered to be sensitive when revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or it contains genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
Regulatory Authority	The National Authority established in each State or per country or per zone which is in charge of monitoring the implementations of Personal Data Protection and Privacy Laws.
Standard Contractual Clauses	The Standard Contractual Clauses (SCC) issued by TSSS at the group level based on the EU Commission or the ad hoc clauses agreed between the Parties and authorized by the Supervisory Authority.
Third country	All States that are not members of the EU or European Equivalent Adequate countries or are not considered by an adequacy decision of the EU Commission as guaranteeing an adequate level of Data Protection.
EEA country	EEA (European Equivalent Adequate) States ensuring equivalent protection to personal data as GDPR protection: Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, and United Kingdom.
Third party	Natural or legal person, public authority, agency or body other than the Data Subject, Data Controller/Data Processor, and persons who, under the direct authority of the latter, are authorized to process personal data.

3 Purpose

With the increase of the use of personal data and the use of new technologies, Privacy is key for TSSS and as a result, the Group Privacy Policy is important as a reference for the entire world where TSSS has its offices, its clients and its employees.

This Group Privacy Policy describes how TSSS entities protect Privacy and personal data. This policy aims to ensure that an adequate level of Data Protection and Privacy is applied throughout TSSS around the world.

4 Scope

4.1 Material scope

This policy covers all privacy matters and personal data processing of TSSS. Material scope includes:

- Human Resources data (past, current employees, job applicant, contractors)
- Connection data (any data related to a connection to a machine)
- Localization data
- Financial data
- Health data, including CIP (Personal Identification Codes)
- Economic data
- Third parties' personal data

4.2 Territorial scope

This policy applies to Spain territory, where TSSS is present and performs business.

At TSSS, we believe that compliance with relevant Privacy laws and Regulations is of utmost importance. TSSS is compliant with the General Data Protection Regulation EC/2016/679 ("GDPR") or any corresponding or similar Privacy laws and regulations worldwide.

5 Personal data protection principles

TSSS personal data strategy is based on privacy by default and privacy by design principles.

5.1 Legal Validity

The legal basis of the processing carried out by TSSS is straightforward and based on the legitimate interest of our entity. For sensitive data, we always request the individual consent for personal data processing.

5.2 Legitimate interest

Data processing is in consideration for the legitimate interests of TSSS, either to improve our Customers' services or the performance of our algorithms or it is demonstrated that the processing is necessary (i.e., there is no better method to measure and evaluate performance that is fair and effective) and proportionate (i.e., only the necessary data is processed).

5.3 Proportionality

Proportionality also requires that the advantages of processing the data are not outweighed by the disadvantages to exercise the right, and that the measure is adequate to achieve the objectives. In addition, when assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed. These standards are met with the use of TSSS services. In addition, policies and processes are applied when using TSSS services: the processing of personal data is systematically ensured to be adequate, relevant and limited to what is necessary for the purposes for which they are processed (i.e. data minimization); Customers are given the opportunity to exercise their rights (i.e. access, correction, erasure and restriction of processing) by, where permitted, effecting changes to data held in the systems constituting the sources of TSSS's data; and personal data is protected by appropriate technical and organizational security measures.

Thanks to TSSS fundamental rights and privacy rules, employees and customers are properly informed of the processing by referring to our appropriate data protection and security policies.

6 Processing personal data

In the course of our business, we may collect and process your personal data for:

- Enabling identity verifications
- Enabling payments
- Managing bank services
- Providing connected or embedded services
- Ensuring security on transportation
- Conducting customer satisfaction surveys
- Complying with our obligations
- Generating statistics and reports
- Marketing purpose with your consent

These processing operations are justified by our legitimate interest or with your consent, to make sure that you enjoy our products and services.

Finally, subject to your prior express consent, we may also use the personal data you share with us for marketing purposes.

7 Data retention

When you are an existing customer, we will keep your personal data for as long as our contractual and/or business relationship lasts. We may then store your personal data in an intermediary database for five (5) years after our contractual and/or business relationship ends.

If you are a prospect with no established contractual and/or business relationship, we will not retain your data for longer than three (3) years after you last contacted us.

If you are an employee, we will retain your data if you are in the company and for 10 years after you leave.

8 Sharing data

We may share personal data within TSSS and with third parties in the legitimate interest of our customers and partners.

We only share data on the contractual legal basis and only for the purpose to serve our customers. Two types of data transfer exist, one within EU or within Austriacard Group, the other outside EU.

8.1 Transfer within Austriacard Group

As TSSS is member of a global organization, Austriacard Group, we have distinct legal entities (e.g., country subsidiaries) in many parts of the world. Therefore, our internal processes and infrastructure are international in scope and nature and generally cross-country borders. Accordingly, you should be aware that we may share your personal data with other entities within TSSS and transfer it to countries in the world where we have data centres or otherwise do business, including those located outside the EU. Such data transfers will be covered by our Data Sharing Agreement (DSA) to ensure the same level of data protection within Austriacard Group affiliates.

8.2 Third-party transfers

We also rely on third-party suppliers and partners with which we may share your personal data for the purposes indicated above, whenever we rely on such third parties, we make sure that they provide an adequate level of protection of the personal data they process on our behalf. When such third parties are located outside of the European Union, we apply the European Union Model Clauses (SCC) as adopted by the European Commission into our agreements.

We also may share your personal data with third parties for marketing purposes, only with your explicit consent.

8.3 Judicial, public and/or governmental authorities

We may also be required – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence – to disclose your personal data to judicial, public or governmental authorities. We may also disclose your personal data if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.

We may also disclose personal data if we determine in good faith that disclosure is reasonably necessary to protect our rights and pursue available remedies, enforce our terms and conditions, investigate fraud, or protect our operations or users.

9 Confidentiality

Confidentiality is key to TSSS activities. We care about confidentiality of the information and expect everyone to respect a high standard of confidentiality.

Confidentiality is not only on TSSS Intangible Assets but also applies to the personal data.

All employees, contractors and partners are committed to respect confidentiality and shall sign a Non-Disclosure Agreement, depending on the situation.

10 Security

Security and Privacy of personal data are a priority for TSSS. Consequently, TSSS implements the necessary measures in accordance with our published Group Security Strategy.

TSSS implements all physical, technical and organizational measures to adequately safeguard the security and confidentiality of personal data for Data Subjects against unauthorized and accidental access, unlawful processing, involuntary or unlawful disclosure, loss, destruction or damage.

11 Cloud

Although, TSSS is not providing any service in the Cloud, in the case this is required, TSSS commits to provide the most secure cloud solutions to its customers according to the relevant applicable laws of each country.

12 Personal data breach

Violations of personal data is managed by our data breach procedure. If the reported breach could potentially damage the rights and freedoms of a Data Subject in a serious way, the Data Protection Officer will notify the relevant national Data Protection authority and, if necessary, inform the concerned Data Subject.

12.1 Communication to the Regulatory Authority

TSSS undertakes to notify the relevant Regulatory Authority of any violation of personal data, as soon as possible, and if possible, within 72 hours after becoming aware of it, except when this violation of personal data is not likely to create a risk for the rights and freedoms of natural persons.

12.2 Communication to Data Subjects

TSSS undertakes to communicate to the Data Subjects any breach of personal data as soon as possible, where such breach is likely to create a high risk for the rights and freedoms of the natural person so that he/she can take the necessary precautions. This communication will describe, as far as possible, the nature of the violation of personal data and make recommendations to the concerned natural person to mitigate potential negative effects. This communication is made in compliance of the Data Protection Authority recommendations.

In general, TSSS does not communicate to the concerned persons when:

- We have implemented appropriate technical and organizational protection measures, and these measures have been applied to personal data affected by the violation, in particular, measures which render personal data

incomprehensible to any person who is not authorized to have access to them, such as encryption.

- We have taken further steps to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialize.
- It would require disproportionate efforts to communicate with the concerned persons. In this case, a public communication or similar measure is carried out which allows Data Subjects to be informed just as effectively.

13 Sub-contracting

TSSS commits to contracting only with sub-processors who provide sufficient guarantees with regards to privacy compliance rules. The carrying out of processing by a sub-processor must be governed by a contract or legal act binding the sub-processor in accordance with the local privacy rules.

14 Data subjects' rights

TSSS commits to respond to requests from Data Subjects without undue delay. Each Data Subject has the following rights:

- To receive a report on his/her personal data in our possession
- To rectify personal data concerning him/her when inaccurate or incomplete
- To delete his/her personal data
- To restrict the processing of his/her personal data
- To object to the processing of his/her personal data
- To ask for data portability according to local privacy laws
- To be excluded from being the subject of an automated individual decision, including profiling

15 Data subjects' requests

Requests from Data Subjects must be sent to the local Data Protection Officer, where the Data Subject is located. These requests can be addressed by postal mail, e-mail or a form available on the intranet site.

The Data Subjects have the right to obtain, within a reasonable period, confirmation that their personal data concerning them are processed or not. The response shall include:

- The purpose of processing
- The categories of personal data concerned
- Recipients or categories of recipients

- The data retention period or otherwise the criteria for determining this period
- The existence of the right to rectification, erasure, and restriction of the processing of their data, and the right to object to such processing
- The right to lodge a complaint with the Regulatory Authority
- The existence of automated decision making, including profiling
- Information about the appropriate safeguards we have in place when the personal data is transferred outside EU

The Data Subject can also send a request to the Group Data Protection Officer at lopd-gdd@atico34.com.

If the Data Subject's request is rejected, the Data Subject has the right to lodge a complaint.

16 Complaints

When the Data Subject has not been satisfied with the response, the Data Subject can submit a complaint or a claim to the Data Protection Authority or to the courts where he/she is located.

17 Cooperation with regulatory authority

TSSS will cooperate with the relevant Regulatory Authority for any questions relating to the interpretation of this policy and will undertake to respond to any queries regarding this policy and its implementation within a reasonable period.

18 Conflicts of laws

TSSS undertakes the processing of personal data in accordance with this policy and any applicable Privacy laws. This policy should be interpreted in the light of any Privacy laws of the country in which TSSS is established.

19 Implementation and review of this policy

This policy is binding on TSSS, its employees, contractors and partners.

This policy is available in English and may be translated into the local language as required.

This policy is a living document that may be periodically updated by TSSS.