DATA PROTECTION

Corporate Policy

CHANGE CONTROL

Edition	**Version 1.0**
Approval date	
Changing sections	
Change description	
Clasification	

INDEX

1. PURPOSE

This Data Protection Policy is the binding basis for legally compliant and sustainable protection of personal data at astara, in relation to compliance with the regulation on personal data protection.

This policy regulates the data protection-compliant processing of information and the responsibilities in this respect at astara. All employees are obliged to comply with the policy.

This policy must be readily available to all Astara's Personnel Scope.

This policy and the current version apply personally to all Astara's Personnel.

The requirements and prohibitions of this policy apply to all handling of personal data, regardless of whether this is done electronically or in paper form. They also apply to all types of data subjects (customers, employees, suppliers, etc.).

2. DEFINITIONS

The following definitions and those of the apply:

- **Affiliate**: means any entity that directly or indirectly through one or more intermediaries, controls or is controlled by the entity specified. For purposes of this definition, control of an entity means the power, direct or indirect, to direct or cause the direction of the management and policies of such entity whether by contract or otherwise, and ownership of the majority of the voting rights of another entity shall create a rebuttable presumption that such entity controls such other entity.
- **ASTARA, Group or Astara Group:** includes Astara Mobility, S.A., and all its, Affiliates and branches
- **Astara's Personnel** meaning all directors and officers, employees, consultants working within or with Astara and workers working at any ASTARA business anywhere in the world.
- **Information and data** are to be understood comprehensively. This includes, irrespective of the content, everything that has been recorded in word, writing, image, sound or in electronic form on any data carrier (paper, hard disk, USB stick, CD-ROM, etc.).
- **Protected data** is all information and data that is collected, processed and managed for business purposes.

- **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an 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.
- **Personal data requiring special protection** is information and data relating to:

    - *religious* (e.g., denomination, payments to a religious community), *ideological*, *political* (e.g., party affiliation) or *trade union views or activities* (e.g., details of attendance at a trade union event);

    - *Health* (e.g., medical dossier, bill for medication), *privacy* (e.g., sexual orientation, information about fears and other feelings, dreams, therapies, medication; but not income and assets) or *racial* (physical characteristics such as main colour) or *ethnic* (e.g., based on shared history or system of attitudes and behaviours);

    - *genetic data* (dann analysis);

    - *biometric data that* uniquely identify a natural person (e.g. fingerprint, iris pattern, facial image; but not body size, eye or hair colour);

    - *administrative and criminal prosecutions or sanctions* (e.g. disciplinary proceedings, driving licence withdrawals, penal measures),

    - *Social assistance measures* (e.g., social insurance benefits in connection with illness and accidents as well as assistance and welfare measures).

- **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.

- **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.

3. PRINCIPLES

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Accordingly, the hardware and software used for data processing shall be used for operational tasks, namely for the respective intended purposes, and shall be secured against loss and manipulation. Use for private purposes requires express permission.

Each employee is responsible for the implementation of the policy in his or her area of responsibility. Compliance must be monitored by him or her on a regular basis.

The persons responsible for the processing of the systems used shall ensure that their employees (users) are informed about this policy; this also applies to temporary employees and external employees.

4. ROLES AND DUTIES

4.1 Responsible

The overall responsibility for data protection in the company is assumed by the company management.

4.2 Corporate Privacy Comittee

Astara has voluntarily appointed a Corporate Privacy Committee whom you can contact using the following contact e-mail privacy.es@astara.com

The Corporate Privacy Committee shall perform its duties free of instructions and using its expertise.

The Privacy Committee has the following tasks/duties in particular:

- **Point of contact**: The Corporate Privacy Committee is the point of contact for data subjects, employees, company management and authorities responsible for data protection in astara. Notwithstanding the above, there is a point of contact for privacy issues per country, (hereinafter the **Privacy Point of Contact**) as follows: TBC (Country/ email address).

- **Training**: The Corporate Privacy Committee supports the company in training employees in the area of data protection.

- **Advice**: The Corporate Privacy Committee advises and informs the company management regarding existing data protection obligations. The Privacy Committee advises the employees and executives on questions regarding data protection.

- **Monitoring**: The Corporate Privacy Committee shall monitor compliance with the Data Protection Regulations, including the requirements of this and other Company policies on data protection.

- **Control**: The Corporate Privacy Committee controls selected processes on a random, risk-oriented basis and at appropriate intervals with regard to their data protection conformity.

- **Reporting**: The Corporate Privacy Committee reports annually in an activity report to the management on audits that have taken place, complaints and any organisational deficiencies that still need to be remedied.

The Corporate Privacy Committee shall be provided with the necessary resources by the management and shall be granted access to all information, documents, lists of processing activities and personal data that the Corporate Privacy Committee requires to perform its duties.
The company or its employees shall involve the Corporate Privacy Committee in all data protection issues at an early stage and support him in the performance of his duties.

5. RECORDS OF PROCESSING ACTIVITIES

The company keeps a register of all processing activities. The Corporate Privacy Committee has the responsibility to compile the necessary information for this purpose on the processing activities of the respective department (e.g., People, Marketing) and to document these in accordance with the legal requirements.

Upon request, the company shall make the directory available to the supervisory authority. In agreement with the company management, the Corporate Privacy Committee shall be responsible for this and shall cooperate with the supervisory authority.

6. COMPLAINT AND NOTIFICATION TO THE PRIVACY COMMITTEE

Every data subject has the right to complain to the Corporate Privacy Committee about the processing of his or her data if he or she feels that his or her rights have been violated.

Likewise, employees may contact the data protection advisor directly with information, suggestions or violations of this policy, whereby absolute confidentiality will be maintained upon request ("whistleblowing").

7. HANDLING PERSONAL DATA

7.1 Collection and processing of personal data

The collection and processing of personal data may only take place within the scope of what is legally permissible. In this context, the special requirements for the collection and processing of particularly sensitive personal data and high-risk

profiling must also be observed in accordance with the legal requirements. In principle, only such information may be processed and used that is necessary for the operational fulfilment of tasks and is directly related to the purpose of processing ("purpose limitation").

The data subject must be adequately informed about the handling of his/her data when his/her personal data is collected ("duty to inform"). The information must include the purpose, the identity of the data controller, the recipients of the personal data and all other information in accordance with the provisions of data protection law, so that the data subject can assert his or her rights and transparent data processing is guaranteed.

If personal data is not collected from the data subject but is obtained from another company, for example, the data subject must be informed subsequently and comprehensively about the handling of his or her data in accordance with the provisions of data protection law. This also applies to changes in the purpose of the data processing.

Personal data must be factually correct and, if necessary, up to date ("accuracy"). The scope of data processing should be necessary and relevant with regard to the defined purpose ("completeness"). The respective department must ensure implementation by establishing appropriate processes. Likewise, data files must be regularly checked for accuracy, necessity and up-to-dateness.

Before introducing new types of collections, the purpose of the data determining the permissibility must be documented in writing by the controller. In principle, a change of purpose is only permissible if the processing is compatible with the purposes for which the data were originally collected. The balancing criteria used in the context of the change of purpose must be examined individually. The examination shall be documented for proper proof.

A change of purpose is also permissible if the persons concerned have been informed in advance.

7.2 Data transmission abroad

The transfer of personal data of European citizens to third parties outside the European Union, the European Economic Area or the applicable country requires special measures to protect the rights and interests of the data subjects. Data must not be transferred if the receiving agency does not have an adequate level of data protection or if this cannot be achieved, for example, by means of special contractual clauses.

7.3 External service providers/contractors (data processors)

If external service providers are to be given access to personal data, the Privacy Point of Contact must be informed in advance.

Service providers with potential access to personal data must be carefully selected before awarding the contract. The selection must be documented and should in particular take into account the following aspects:

- Professional suitability of the contractor for the specific handling of data
- Technical-organisational safety measures
- Experience of the provider in the market
- Other aspects that indicate reliability of the provider (data protection documentation, willingness to cooperate, response times, etc.)

If a service provider is to collect, process or use personal data on behalf of a client, a contract for processing the order must be concluded. Data protection and IT security aspects must be regulated in this contract.

The service provider shall be reviewed regularly with regard to the technical and organisational measures contractually agreed with it. The result shall be documented.

7.4 Data minimisation, Privacy by Design/Privacy by Default

The handling of personal data shall be geared towards the goal of collecting, processing or using as little data as possible from a data subject ("data minimisation"). In particular, personal data must be anonymised or pseudonymised as far as this is possible according to the purpose of use. For example, in the context of a statistical evaluation of data, it will not be necessary to know and use the full name of a data subject. Rather, this information can be replaced by a random value, which can also ensure that the underlying information is distinguishable.

The same applies to the selection and design of data processing systems. Data protection shall be integrated into the specifications and architecture of data processing systems from the outset in order to facilitate compliance with privacy and data protection principles, in particular the principle of data minimisation.

8. RIGHTS OF THE DATA SUBJECT

The person concerned shall be informed within 30 days at the latest of any measures taken at his/her request.

The Privacy Point of Contact is available to advise on the protection of data subjects' rights.
Astara Group, as the data controller, will facilitate the exercise of the data subjects' rights of access, rectification, erasure, limitation of processing, portability and objection, establishing the necessary internal procedures to satisfy the applicable legal requirements. In this regard, it shall make it possible to submit requests in a

simple manner, by electronic means, especially when the processing is carried out by these means.

9. TRAINING

Employees who have permanent or regular access to personal data, collect such data or develop systems for processing such data shall be trained in an appropriate manner on the requirements of the applicable data protection regulation.

The Corporate Privacy Committee shall decide on the form and frequency of the relevant training.

10. DATA SECRECY

Astara's personnel are prohibited from collecting, processing or using personal data without authorisation. All employees must strictly observe the principles of data protection legislation, namely the internally issued directives and guidelines on the protection of information and data.

11. AUDITS

In order to ensure a high level of data protection, relevant processes are reviewed through regular audits by internal bodies or by external auditors. In the event that potential for improvement is identified, immediate corrective measures are to be taken.

The findings obtained during the audit shall be documented. The documentation shall be handed over to the Corporate Privacy Committee, the company management and the persons responsible for the respective process.

An audit is successfully completed when all measures documented in the report have been implemented. If necessary, follow-up audits are carried out by reviewing the implementation of recommendations from the initial audit.

12. INTERNAL INVESTIGATIONS

Measures to clarify the facts and to avoid or uncover criminal offences or serious breaches of duty in the employment relationship must be carried out in strict compliance with the relevant statutory data protection provisions. In particular, the associated collection and use of data must be necessary to achieve the purpose of

the investigation, appropriate and proportionate with regard to the interests of the data subject that are worthy of protection.

The person concerned shall be informed as soon as possible of the measures taken in respect of him or her.

13. DATA SECURITY

In order to safeguard the confidentiality, availability, integrity and traceability of data, a general security concept is drawn up, which is binding for all procedures. In particular, the state of the art must be taken into account, as well as means and measures for encryption and data protection. The security concept must be regularly reviewed, assessed and evaluated with regard to the effectiveness of the technical and organisational measures provided for therein.

14. DATA MANAGEMENT

Data is always stored on the network drives provided for this purpose. Storage on mobile data carriers or cloud storage requires the approval of the IT department and registration by the department/user using the carrier. In the case of networks, the IT department is responsible for backing up the data stored on the server.

If a different storage location is required for technical reasons (e.g., notebook, desktop PC), the respective user is responsible for performing the data backup. If network access is possible (e.g. notebook with WLAN, tablet), the current data must be transferred to the network drive reserved for the user at least once a week.

Legal retention periods and deletion deadlines must be observed. The IT department shall be informed of compliance with the deadlines, especially with regard to the deletion of personal data in backup copies.

When IT components that are no longer required are passed on or returned, the user is obliged to ensure that all data has been effectively deleted beforehand.

15. DATA PROTECTION IMPACT ASSESSMENT

The Privacy Point of Contact is obliged to carry out data protection impact assessments for procedures that take place under its responsibility if a processing operation may entail a high risk to the personal rights or fundamental rights of the data subject. The data protection impact assessment contains all descriptions required by law.

A data protection impact assessment shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

16. VIOLATIONS OF THE PROTECTION OF DATA ("DATA BREACH")

Every employee is obliged to immediately report malfunctions, security incidents and emergencies in the area of information security and incidents in the area of data protection to the Privacy Point of Contact and to the CISO ciso@astara.com

The notification shall include all relevant information to clarify the facts, in particular the receiving agency, the data subjects and the type and scope of the data transmitted.

The fulfilment of any duty to inform the supervisory authority shall be carried out by the Privacy Point of Contact, previously approved from the Corporate Privacy Committee.

17. FINAL PROVISIONS

- **Consequences of infringements**

A negligent or even wilful breach of this policy may result in action under employment law, including dismissal with or without notice. Criminal sanctions and civil consequences such as damages may also be considered.

- **Accountability**

Compliance with the requirements of this guideline must be verifiable at all times. In this context, particular attention must be paid to the traceability and transparency of the measures taken, for example through the corresponding documentation.

- **Updating the policy; verifiability**

In the context of the further development of data protection law as well as technological or organisational changes, this guideline will be regularly reviewed to determine whether it needs to be adapted or supplemented.

Amendments to this policy shall be effective informally. Employees and officers shall be notified of the amended requirements immediately and in an appropriate manner.

18. REFERENCES

This policy is part of the regulations on data protection. This policy is overridden by laws and regulations, while various other internal regulations and documentation follow and implement this policy. For example:

- Ethis Code
- Technological Media Use Policy
- Suppliers Code of Conduct

Such supplementary internal regulations and documentation may include, in particular, the realisation of the data protection and data security measures to be taken. These include, among others, the staff regulations and the data protection declaration.

Should an objection arise, the following order of precedence shall apply:

- Laws and regulations
- This data Protection Policy
- Further subordinate internal regulations and documentation

If necessary, the documents are to be adapted immediately in the sense of the superordinate provisions.