SECURITY MEASURES

The safety requirements in this document are intended to comply with current legislation, that is at D.Lgs 196/2003 as amended by D.Lgs 101/2018 and REG.UE 2016/679 regarding the processing, protection and circulation of personal data.
A.I. Tech reserves the right to check the effective application of the security measures defined through periodic checks.
This document consists of a description of the model adopted by A.I. TECH, with specific reference to the elements of compliance with the regulatory principles and the model by design, and to a list of measures adopted to guarantee confidentiality, availability and resilience of systems and treatment services.

Description of the technical and organizational security measures implemented (art.32 EU REG. 2016/679)

The technical and organizational security measures reported in this document are implemented, applied and kept constantly updated, in addition to the further measures required to guarantee and ensure a level of security appropriate to the risk, taking into account the state of the art and the costs of implementation, as well as the nature, the scope , the context and the purpose of the processing, together with the risk of varying probability and severity for the rights and freedoms of natural pers ons.

Approach by design art. 25 GDPR

Before making a product operational, the design phases are documented, in particular considering the development only for the data to be treated (minimization principle).
Products / applications are identified, the mode of operation and architecture, the technical documentation to support, detection / mapping of the data collected by the system and their possible use.
Together with the aforementioned steps, it is possible to confirm the implementation of privacy by design and by default, to have as a support the user manual, the test documentation and verification tests.

The video analysis solutions of A.I. Tech and security measures

Video analysis solutions require data collection, data processing, data use and data sharing and must respect:

- the principle of transparency;
- the adoption of adequate technical and organizational security measures to guarantee an adequate level of security to the risks;
- the data must be, when possible, minimized, anonymised or pseudonymised;
- it is necessary to identify a limitation of the purposes (use of data for purposes compatible only with the purposes to be pursued);

- the rights of the interested parties must be protected;
- the configuration of the techniques and procedures relating to the methods of treatment must be guaranteed so that the criteria that are considered from the initial stage of a project are clear and so that data security is guaranteed with a privacy by design approach.

They are therefore guaranteed by A.I. Tech the following principles:

- lawfulness, fairness and transparency;
- personal data are collected only for a specific purpose, or for the purposes declared and with a conservation criterion respectful of regulatory requirements;
- the data can be minimized according to the principle of privacy by design and by default, only the personal data necessary to achieve the purpose for which they are processed will be processed.

Even in the case of "biometric" detection, no personal data remains permanently stored in the system; the images are neither saved locally on the device nor transmitted to other systems, unless the user decides, through explicit consent and a specific configuration on the system, to save the images related to the events generated by the system, with the metadata associated with it, for example activating the saving of images on AI-DASH-EMBEDDED or sending in AI-DASH-PRO. With regard to the classification of the images (for example for the face -analysis), no image associated with people's faces is stored in any way (except in case of an explicit consent of the operator, as mentioned above). The face is encoded in a vector of salient characteristics (not attributable in any way to the face itself and therefore to the identity of the person), and processed in real time through the use of classifiers, i.e. complex mathematical models that given this vector are able to detect for example the gender or age of that subject.

The accuracy of personal data is an integral part of their protection as it is guaranteed thanks to the integrity and confidentiality security measures.

The A.I. Tech model

- Description of the treatment: Each solution is presented with a description with respect to the features that represent the description of the treatment and the purposes that can be pursued.
- Assessment of necessity and proportionality: the adoption of the solution on the basis of the identified purposes may be justified according to the context, the objectives and also considering the need for analysis allowed by the algorithms made available with an intelligent detection system.
- Measures taken to demonstrate compliance: the safety measures guaranteed and reduced in the individual application methods of A.I. Tech solutions allow you to define the conditions of adequacy for the purpose of the evaluation to be carried out.

- Assessment of the risks for the rights and freedoms: in the face of the risks for the rights and freedoms of the interested parties, the solutions respond to the users' purposes and can also be installed and implemented, guaranteeing security measures and the minimization and anonymization of data or pseudonymisation.
- Measures foreseen to face the risks: A.I. Tech guarantees the application of the measures required by current legislation which may be subject to evaluation activities for the purpose of correct analysis and management.
- Documentation: the use of the solutions is supported by the necessary documentation which in turn allows Users to be able to define the evidence and the documentary supports to confirm their accountability.
- Monitoring and review: the measures put in place and the model built on the basis of the specific solutions and guarantees made available allow the necessary monitoring and control activities also to be able to face any vulnerabilities and intervene to improve the effectiveness and efficiency of the systems themselves.

ANONYMIZATION AND PSEUDONIMIZATION

The collection of information carried out through systems and sensors is aimed at measuring and personalizing the customer experience and pursuing a whole series of organizational and security reasons. The information is processed by coding the image in a numerical descriptor and in any case in a given anonymous information that represents the parameters / events detected. The descriptor is obtained through a transformation that will no longer have any correlation with the information managed on the systems. No data is recorded or stored or memorized unless explicitly requested by the user during configuration, through the explicit saving of images relating to the event of interest in AI-DASH-PRO or AI-DASH-EMBEDDED (dashboard for management of events integrated in the application).
Access to the configuration module, as well as to the data stored in the dashboards, is guaranteed through the standard authentication mechanisms provided by the HTTP protocol (via username and password), therefore it is not possible to access these confidential data without credentials.

A.I. Tech ensures:

Anonymization: Personal data are processed so as to avoid the person concerned to be identified.

Pseudo-anonymization: Even if the user requires to store the stream, it is possible to apply policies to reduce the risk to relate the extracted data to the original identity in the scene (eg. divide the stream from the data extracted). For instance, it is possible to store the stream on a third-party Video Management System and collect the data extracted by analyzing the stream on AI-DASH-PRO without the possibility to relate the information stored on both the systems to the person in the scene.

In addition to the measures and principles mentioned above A.I. Tech guarantees the following technical and organizational security measures:

Backup

Data availability and data recovery are guaranteed through dedicate backup procedures. The effectiveness of these procedures is periodically checked through backup verification and recovery tests.

Business continuity and disaster recovery

Considering the repository software, disaster recovery procedures and security measures are defined and implemented. Furthermore, disaster recovery plans are regularly tested, at least annually, in order to verify their effectiveness;

A continuity plan is implemented to guarantee the compliance with the contracted defined service levels (SLA), to guarantee the service even in case of emergencies.

End-to-end data protection

Secure transmission protocols are implemented through protected communication channels for the transmission of data between the platforms and the systems concerned as well as for the transmission of data between the platforms used to provide the services.

Encryption mechanisms are used for the transmission of data and information at least at the file level as per international standards

Data protection

Security measures are implemented for the data stored or collected by servers and databases, such as disk level encryption, according to the international security standards.

Development, test and production environments are isolated from each other in order to reduce the risk of unauthorized access or modifications.

Perimeter security

Perimeter security measures (e.g. Firewall,) are adopted to protect the network and devices (e.g. server, database) supporting the provided services.

Access management of authorized users and administrators

An access model is defined with a list of administrators and their individual privileges within applications or data collections. The use of a multi-factor authentication systems is required for all the administrative accesses. If the multi-factor authentication cannot be adopted, it is required the use of user credentials respecting to the strongest international security standards.

Security event management

An incident management process has been implemented in order to: detect, analyze, classify anomalous events according to their level of severity and react adequately to potential internal and external attacks.

Hardening e Patching

Periodic hardening and patching activities are performed to all the systems supporting the software development process.

Activity tracking

Access log are store and monitored. It is possible to trace the activities of staff users with special privileges (e.g. administrative users) through access and activity logs.

Anonymous administrative users are used only for emergency situations and the related credentials must be managed in order to ensure the identification of those who use them.

In any case, unique identities and passwords are assigned for the purpose of managing user access. Individual identities IDs cannot be shared.

A.I. Tech provides the following additional measures:

Security policy

A security policy has been defined together with periodic reviews and updates.

Minimum privilege principle

There is no way a person can perform activities that could create security conflicts ("segregation of duties", for example: developer / reviewer, developer / tester).

Access privileges are constantly updated and made consistent with the role played by a user within the organization, in case of job change, resignation or dismissal they are promptly updated and / or revoked.

Training

The team members are trained concerning data security.

Destruction of hard copies

In the case of the use of paper documents, the destruction of the hard copies containing data in a non-reversible way is adopted.

Change Management

In the case an employee changes his job / role due to resignation / dismissal, access to offices and applications is denied if no longer necessary.

Information and deliverable reuse

File and information sharing outside the project team and / or development environment are monitored.

Data deletion and destruction

In any case, it is performed the deletion, using secure methods, of electronic files and / or devices containing confidential or strictly confidential data after the data are no longer necessary and in case that the devices are no longer used.

Encryption and data retention

Disk level encryption mechanisms are applied to all physical workstations used to process data.

Servers containing the source code repository, project documentation and internal documents are secured using file-level encryption mechanisms according to international security standards in order to keep confidential or strictly confidential data outside the application environments.

Only encrypted devices are used to temporarily hold the data and verify that the data is permanently deleted when it is no longer needed.

Physical security of IT equipment

Security controls are implemented to ensure the security of the IT equipment to avoid tampering and / or theft.

Cloud data management

The following measures are adopted in order to manage data on the cloud:

- risks and benefits of using the cloud
- cloud computing provider reliability
- physical server housing
- contractual clauses to guarantee the type of data treatment

- data retention
- service security
- organizational measures (e.g. training) for staff responsible of using the platforms

Use of IT resources:

- There is no unauthorized or non-compliant processing of data related to the use of the applications
- There are no treatments that can in any way impact on the confidentiality, availability or confidentiality of the data
- Exports of any kind are not allowed
- Configurations cannot be changed in any way unless expressly requested or explicitly approved