Author	Privacy Department (Zucchetti Spa)/Development Manager
Approval	Management

Revision version

Version	Author	Consultation of DPO	Issuance date	Reason for the revision
0.0	Privacy Department (Zucchetti Spa)/Development Manager	24/05/2018	25/05/2018	First issue
1.0	Privacy Department (Zucchetti Spa)/Development Manager	18/06/2019	19/06/2019	Versioning added; the purpose of the processing has been changed
2.0	Privacy Department (Zucchetti Spa)/Development Manager	07/10/2019	07/10/2019	Description of new security functions
3.0	Privacy Department (Zucchetti Spa)/Development Manager	13/12/2019	13/12/2019	Support procedures added
4.0	Privacy Department (Zucchetti Spa)/Development Manager	05/11/2021	10/11/2021	Reference to the functionality related to Green Pass validation added
5.0	Privacy Department (Zucchetti Spa)/Development Manager	13/01/2022	13/01/2022	Log deletion times added
6.0	Privacy Department (Zucchetti Spa)/Development Manager	20/01/2022	21/01/2022	Details related to XPOINT and FM added
7.0	Privacy Department (Zucchetti Spa)/Development Manager	29/02/2024	29/02/2024	The Data Centre support and security measures have been updated

OPINION OF DPO
OK.

ZUCCHETTI SERVICES AND PRODUCTS RELATED TO GDPR PROVISIONS: XATLAS (*as of version 1.9.20*)

DATA PROCESSOR					
Name	Zucchetti Axess S.p.a.				
VAT no.	03537610960				
Address	Via Solferino, 1				
City	Lodi	**Postal code**	26900	**Prov.**	LO
Legal representative	Domenico Uggeri				

ORGANISATIONAL STRUCTURE			
Division	XATLAS	**Division Manager**	Domenico Uggeri
Area	XATLAS	**Department manager**	Marco Marchetti

PERSONS IN CHARGE OF PROCESSING
Analysis, development, quality control and help desk operators.

CONTACT DATA			
Data Processor	Zucchetti Axess Spa	Ufficio.privacy@zucchetti.it	0371.5947000
Representative of Data Processor	N/A		
Data protection officer (DPO)	Mario Brocca	dpo@zucchetti.it	0371.5943191

DESCRIPTION
XATLAS is a security management platform for managing access control, security of individuals, attendance data collection, anti-intrusion, fire-fighting by interfacing with fire alarm control panels, video surveillance by interfacing with cameras via IP or milestone, and for passing information to other applications for managing meals in company canteens. Within XATLAS, it is possible to activate a specific functionality related to the validation of the green pass, which is carried out through a solution developed directly by Zucchetti Axess. No data is saved except for the QR CODE for the time strictly necessary for the verification itself to authorise access to the gate.

PURPOSE OF THE PROCESSING
Management of access control, both of vehicles and individuals; management of security of people and property. The purpose of the processing is to provide support and maintenance services to the Data Controller.

CATEGORY OF INTERESTED PERSONS
Employees, collaborators, visitors, vehicles in the Xatlas Master Data.
CATEGORIES OF PERSONAL DATA
Personal data: identification data, accesses to gates and transits of persons and vehicles. *Special categories of personal data*: personal data presenting specific risks will not be processed. There are blank fields in which the Data Controller may enter personal data that is contextual to the application purposes, the contents of which we do not know. The software can work by interfacing with card-based biometrics hardware systems or database-based biometrics where the fingerprint also resides on the Xatlas database. This second category is only sold on the foreign market. XAtlas can be sold in cloud (more details on how to sell)
CATEGORY OF RECIPIENTS TO WHOM DATA CAN BE COMMUNICATED
Subcontractors/sub-suppliers, if the communication is necessary to fulfil contractual obligations for the purposes of application support and maintenance.
DATA TRANSFER ABROAD
The data transfer abroad is not provided by the Data Processor.
RETENTION PERIOD
Data is retained for the entire duration of the contract and, following its termination, the entire software remains available to the customer for the next 90 days. At the end of this period, a 12-month retention period begins for backup copies.

1. TECHNICAL MEASURES THAT CAN BE IMPLEMENTED AT APPLICATION LEVEL

- *Authentication system*:

Xatlas has various authentication methods:

1) with login and password;
2) configurability with SITEMINDER (SSO mechanism);
3) the customer side can be integrated with the Windows user. The login page can be authenticated by Xatlas or it can rely on a page that does ldap.

If the login and password are configured by Xatlas, there are various configurations of both complexity and maximum reuse, in particular:

Password and username rules: minimum length, how often to change it, it is possible to provide temporary passwords with compulsory replacement at first use, reuse of passwords already used is forbidden, controlled number of consecutive errors of incorrect typing of passwords with blocking of access attempts, user not used for at least 6 months disabled, the same user cannot be used at the same time by two different stations, passwords saved in db with SHA 256 encryption, configurability in terms of complexity so they must contain at least a number, upper case, lower case and special characters. After some time of inactivity of the system with active log in, the system autonomously interrupts the session.

- *Function to extract data in a structured format* ***(right to portability):***

timestamps can be exported in csv format. The generated data either remain on the system or they are sent over SFTP or WEB service areas, or they can remain on the db and transferred with a direct connection to other databases. Every scheduled operation or made by the operators is scheduled by an event log. If the operators generate a csv, the information is saved in the log. When an employee, customer, visitor requests the access right to data, an extraction in json format is performed, with which the data on the system will be provided.

- *Registered user for system administrators:*

the customer is given a default administrative user which s/he must change and keep secret. The choice of the individuality of the generated user and of the assigned access profiles is left to the customer.

- *Support for verifications provided by GDPR*:

with appropriate data extractions, both operators and access profiles can be printed from the system

- *Predefined profiles for the most common operator roles with restricted access rights* (***privacy by default***):

the customer is given the admin operator and the guest operator that is read-only. With the admin user, the customer can generate an operator with admin rights with which to configure all other users. The admin user, when used, can be made unusable by the customer. In Xatlas, roles such as lab operator, technician, security operators, HR operators and receptionists are predefined, so that the customer can already have standard configurations and does not bear the risk of making incorrect configurations.

- *Deletion of personal data* (***Right to be forgotten***):

data can be deleted in two macro-categories: there is always data and time-related data. Data can be deleted or archived. In the start-up phase, the customer can decide which data to store, where to store it and after how long to delete it; it is possible to set the explicit end of use on the Master Data, which is a date that, if set, allows a series of data to be deleted in a way configurable by the customer. The customer chooses the deletion methods autonomously. These functions are processed on employees, outsourcers, vehicles and their timestamps.

- *Anonymisation:*

all logins and passwords to other systems are saved in SHA256. Personal data is not anonymised, but it is directly deleted at the end of its life according to the previous paragraph.

- *Logs*

The logs record the log in, log out, and any operations that are done writing or activating commands. Logs are kept for 24 months if in db or txt format when they reach a size of 1 mega. When they reach this size, txts are renamed up to a maximum of 10 times. It is up to the customer to save them in another repository if s/he wishes to keep them longer.

- *Blurring LOG files:*

by default, they are unencrypted, but it is possible, upon the customer's request, to configure an encrypted log. Registration takes place as described above.

- To ensure continuity of service, the DB is agreed with the customer as a cluster and there is the possibility of redundancy of nodes. FM guarantees continuity of service for the collection of timestamps even if the network and connectivity is temporarily interrupted.

- *Change management*:

RQS are assessed and it is decided whether to enter them in the system and develop them. The procedure is assessed by the application development manager.

FM and XPOINT side (hereinafter referred to as FM for short) and terminals.

In particular, we can list the following macro items:

- A prerequisite is that the specific terminal has a firmware implemented with the changes for GDPR; however, FM is capable of handling mixed scenarios;
- FM automatically recognises whether or not the firmware of the individual terminal supports encryption and then, without any special configurations, it automatically sets itself to “GDPR security” configuration;
- Management of anonymised biometrics template sending: both sending and receiving of fingerprint templates are blurred. FM anonymises before transmitting and does the opposite job on the receiving end. In this case, no data is left on the terminal filesystem, which only acts as a gateway to the sensor DB;
- Management of anonymised user table: the management on FM is similar to the one of biometrics, but in this case a trace remains on the terminal if the table is anonymised or not;
- Blurring of log files: on FM, as well as on XAtlas, it is possible to blur the log files by editing the *log4j* configuration file and properly setting the appender that manages the encryption. Obviously, where this setting is made, the logs are unreadable and their decoding can only be done by R&D on the received affected file.
- Secure communication protocols: terminals can be configured to communicate only in https format. The customer decides in the start-up and configuration phases. Data is exchanged via file manager on Linux machine or directly in FM with proper proprietary DB so that it resides autonomously even if disconnected from the network. FM stores data according to the number of timestamps configured by the customers.
- encrypted file exchange: the customer chooses whether to encrypt in Https or not

The above security functions are not active by default. The Data Controller will make the necessary configurations to activate the proper risk mitigation functions.

With regard to the security measures of cloud services, please refer to the security measures declared by the service provider.

2. DATA PROCESSOR: SUPPORT PROCEDURES

SUPPORT SERVICE METHODS

Based on the supply method, the support for Zucchetti Axess products and services is provided in the following ways:

- On-site support
- Telephone support
- Support via e-mail/web tickets
- Support by importing customers' database
- Support via remote connection
- Support via remote VPN connection

CONTRACTORS TO WHOM THE SUPPORT SERVICE IS PROVIDED

The support service is provided to:

- Direct Zucchetti Axess customers
- Indirect customers

The support management generally provides:

- for direct customers: telephone call or e-mail to the service department (back office/dedicated mailbox) which sends an e-mail to the support department. The call is opened on V-Tiger;
- for indirect customers, the request is sent directly by the customer to a dedicated mailbox (support@axesstmc.com).
-

PROCEDURES

ON-SITE SUPPORT

Zucchetti Axess operators access the customer's structure in order to carry out training or technical maintenance/support and installation activities.
In this case, they work as if they are part of the Customer's/Data Controller's structure and they adopt all the procedures required by the Customer. The Customers/Data Controllers can generate individual user names for accessing their systems or they will provide access under supervision to Zucchetti Axess appointees in order to train their staff.

TELEPHONE SUPPORT

There are no issues as far as the personal data processing is concerned. There are no transmitted data or archives and the communication is only verbal. Generally, the first contact after the customer's request for support is always made in this way, in order to define the reported issue in detail.

SUPPORT VIA E-MAIL/WEB TICKETS

In case of support via e-mail, always add the disclaimer in the message text:
"The content of this e-mail and of possible attachments is strictly confidential, it is not admissible in court and it is dedicated to the person/s to whom it is addressed. The content of the reply to this e-mail might also be known by other co-workers, who are part of the same homogenous group of the undersigned or part of other homogenous groups who are however related to the solution of the issue reported by you. If you received this e-mail by mistake, please notify us immediately and delete it from your computer. It is prohibited to copy and publish the content of this e-mail. Any abusive use of the information contained here, by third parties or by persons who are not indicated in this e-mail, can be prosecuted pursuant to the law. We hereby inform you that in order to exercise the rights provided by article 15 et seq. from the EU Regulation 2016/679 (GDPR), it is possible to refer to the following address: ufficio.privacy@zucchetti.it".

Zucchetti Axess appointees must never have the customer's access credentials sent by e-mail (only those used and in the possession of the customer, not those generated specifically for technicians who need to connect), nor must they save them on the ticketing tool and/or in e-mails.

If a customer/partner sends the access credentials for his/her environment without a request from Zucchetti Axess appointees, it is necessary to reply them that we are not authorised to access the systems with other users' credentials because this method infringes the EU Regulation 2016/679 (GDPR). Therefore, Zucchetti AX appointees will have to request individual credentials or the remote connection.

Every e-mail must be signed with the first and last name of the operator who handled the Customer's issue and the information must be saved in the ticketing tool and/or in the e-mail.
Clarifications:
The disclaimer can also be added in the web tickets.
Personal e-mail addresses should not be used, as they cannot be controlled.

SUPPORT BY IMPORTING CUSTOMERS' DATABASE

If, in order to solve the issue reported by the Customer/Data Controller, it is necessary to have the database or other files or queries containing personal data transmitted, the Customer must be informed of this necessity. If the customer is not able to make the copy himself/herself and asks Zucchetti Axess appointees to do so, it is necessary to receive his/her authorisation also for the VPN connection (to be saved in the ticketing tool and/or in the e-mail).

In order to carry out this activity, it is necessary to send the customer/Data Controller an e-mail with the following content:
”Dear Customer,
in order to solve the issue reported by you, it is necessary to check your archives.
We ask you to authorise us to connect via VPN to take copies and to process them in order to solve what has been reported”.

The archives will be stored for the time strictly necessary to solve the reported issue and will be deleted by Zucchetti Axess appointees at the end of the intervention.
Data must be saved in the Directory and they should not be subject to backup”.

If there is the need to store the archives, it is necessary to send an e-mail to the customer, as described below:
“Dear Customer,
having solved the issues on the archives that you sent, we request the authorisation to store your archives on our infrastructure for the next _____ days. The purpose of this storage is to check for possible issues that you may report during the use of the restored archives. At the end of the above-mentioned period, we will proceed to the permanent removal of the archives. If after this period your archives are needed, we will request them again.
To this end, we request an express confirmation by replying to this message. If your reply is negative, we will proceed to the immediate deletion of your archives”.

The customers' archives cannot be transmitted to work groups other than those in charge with solving the issue reported by the customer.

The only possibility to store the archives without the prior authorisation of the customer is to make them anonymous.

SUPPORT VIA REMOTE CONNECTION

This method of connection to the customers' tools ensures privacy because:
- The connection is always requested by the customer
- The access credentials are always individual

- The customer grants us access to an environment with an authorisation profile chosen by him/her in order for us to perform support activities
- The customer can disconnect us whenever s/he wishes.

Via the remote connection, it is also possible to grant access for the second level support to the same session opened by us. In this case, the customer has the proof as it has been provided by the tool and therefore s/he implicitly accepts this method.

SUPPORT VIA VPN CONNECTION

If the support activity must be performed via VPN or private accesses, Zucchetti Axess operators must enter the customers' systems:

- With the customer's prior authorisation
- With the credentials that must be active for the time frame needed for the execution of the requested activities
- The credentials must be disabled at the end of the activity by the Customer/Data Controller

The creation of a user name must only be requested from the customer, who must generate it individually for every Zucchetti AX appointee.
The users are generated by the customer during the initialisation phase of the agreement and remain active for its entire duration.

At the end of the support activities, Zucchetti Axess technicians notify the customer that the support activity has been concluded.

SUPPORT FOR VIDEO SURVEILLANCE

The support for video surveillance systems is first carried out remotely to check the issue.
If the video camera cannot be reached remotely, the support is carried out on site.
The technicians never access the records, unless expressly requested by the customers.

SUPPORT DURING THE TESTING PHASE

If it is necessary to carry out tests on the customer's DB, Zucchetti Axess staff will run them on the customer's systems, on a new machine/server put at disposal, which will then be used for production once the tests are completed

3. DATA PROCESSOR: SECURITY MEASURES APPLIED TO THE DATA CENTRE

As part of the service supply, Zucchetti Axess makes use of the Data Centre provided by AWS.
Certifications: Zucchetti Axess considers security as a primary and indispensable element for the company and for its own customers and that is why it has organised its own management systems, which comply with strict security criteria. The organisation of a management system entails the creation of roles, activity flows and clearly defined procedures governing the company processes. Certifications: ISO 9001 and ISO 27001
Compliance: Zucchetti Axess company processes meet the regulations in force, especially as far as the compliance with the privacy requirements is concerned. In this context, the company has already adapted its management system to the requests of the Data Protection Authority's order on system administrators. If the legal regulations are amended, Zucchetti Axess will immediately adapt to the method of supplying the service and the technical specifications in order to make it compliant with any amendments.
Access to information: Zucchetti management system allows the clear classification of the privacy level of each document. Especially the documents containing information on the security systems are classified as private and are not disclosed outside the company.
Access to the systems: the accesses to systems can always be classified in production accesses and administration ones. Production accesses are subject to the service supply. Administration accesses are those performed by Zucchetti Axess or by the customer with different purposes, such as maintenance, error checking, data acquisition. Zucchetti Axess administration accesses are reserved to the staff having the qualification ("role") of system administrator. The company focuses especially on the assignment of that role

only to staff having high technical skills and having proven qualities of reliability and morality. The administrative access to the systems performed by the customer's staff will take place through nominal assignment of the staff to roles to which access privileges are assigned.

Auditing: within its own management system, Zucchetti Axess especially focuses on the audit of the systems and administrative activities carried out on them. The AWS infrastructure is configured to report its own logs to a centralised processing, classification, repository and alerting system (CloudWatch). Both single events and patterns of infrastructure malfunctioning (e.g. overloads) can be detected. The log management and analysis systems are moreover used for monitoring the activities of the system administrators as prescribed by the order of the Data Protection Authority. The access to the log management system is reserved to Zucchetti Axess staff.

Data privacy: this document was drawn up by assuming that the data collected from the customer and available on the host systems within the Data Centre are of personal/sensitive type, according to the classification provided by the Personal data protection code.
In each case, Zucchetti will not process the customer's data, except for the sole purpose of their storage. Zucchetti Axess will not be able to know in any way the Personal Data added by the customer unless authorised by the him/her for the purpose of performing environment maintenance and support activities. Zucchetti Axess does not assume any liability for the use of such data by the customer or by the companies appointed by the customer that manage or use the service housed and managed in the AWS Data Centre. Zucchetti Axess will manage and store the information in compliance with the regulations expressed by the law in force.

Log Management: the system logs contain information necessary for the administrative, diagnosis and security activities. Each system is configured to log every significant event. The logs generated by each system are transferred to a central repository that has the task to analyse, classify and store. The log storage occurs according to the legal regulations, especially the Privacy Code and the regulations on the storage of the telephonic and electronic traffic data. The systems logs contain all the significant activities for security purposes, such as administrative accesses, permission changes and other system and security configurations, anomalies. These logs are stored with the same system log methods. In particular, all access and administrative activities are traced and archived according to Guarantor's measures on Personal Data Protection of 27th November 2008 on system administrators.

Security controls: penetration tests and vulnerability assessments are performed annually on the entire infrastructure.

Firewalling: the networking of the Data Centre is separated from public networks, from other Intervieweb networks and from other customer's networks. The data flows between the Data Centre networking and the outside world are mediated by firewall systems. Those firewall systems allow the transit only to the data flows that are necessary for the operation of the service and explicitly authorised. The systems used for networking isolation are: Virtual Private Cloud (Aws VPC), Security Groups (Aws), NAT, LoadBalancers.

Intrusion Prevention: the Data Centre is protected by Intrusion Prevention Systems (IPS) that allow analysing the entire entrance traffic, immediately identifying the attack attempts in progress. The network traffic on significant segments of the platform passes through systems that inspect each pack of the transit traffic and behave in a transparent way when meeting legitimate traffic.

Filesystem Antivirus: all servers have Antivirus modules on the file system and, on a project base, specific antivirus products can be configured and centrally managed in terms of update, policy distribution, launching of scans on demand, notifications and management of the quarantine area.

Security Patch Management: the platform is subject to a periodical verification process of the patches and fixes released by the manufacturer and considered critical for the service supply and for the security.

ACCESS TO SERVERS

Access to the incoming servers is via key exchange (RSA-256 Public/Private).
Each system administrator has his/her own SSH access key and nominal user.
Such user does not have administrator privileges.
If it is necessary to acquire higher rights, there is the possibility of scaling up to an administrator user.

Every attempt to access the operating system (accepted or failed) is logged as well as any user escalations and commands sent.

BACKUP

All databases are backed up twice during the night.

1. Daily automatic backup provided by the RDS-AWS service
2. Daily automatic backup on the file system of the server hosting the software

CERTIFICATIONS OF AWS DATACENTRE

ISO 9001 – ISO 27001 - ISO 20000 - ISO 23301 - ISO 27017 - ISO 27018 - ISO 277001