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

Revision version

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

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	+39 0371.5947000
Representative of Data Processor	N/A		
Data Protection Officer (DPO)	Mario Brocca	dpo@zucchetti.it	+39 0371.5943191

DESCRIPTION

XATLAS is a security management platform for managing access control, security of persons, 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.

PERSONAL DATA CATEGORIES

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 biometrics hardware systems or database 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 THE 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 OUTSIDE THE EU

No.

1. TECHNICAL MEASURES THAT CAN BE IMPLEMENTED AT APPLICATION LEVEL

- *Authentication system*:

Xatlas has various authentication methods:

1) with login and password;
2) set to be configured with side minder (sso mechanism);
3) the customer side can be integrated with the windows user. The log in 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:
<u>Password and username rules</u>: 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 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 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 users 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 users and 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 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 are predefined, which are lab operator, technician, security operators, HR operators and receptionists, 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. The customer in the start-up phase can decide which data to store, where to store it and after how long to delete it; on the Master Data, it is possible to set the explicit end of use 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 operation that is done to write or activate 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 of 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 special 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 via customers' database import
- Support via remote TeamViewer and/or Meeting Webex connection
- Support via remote VPN connection
- Start-up projects and conversions

As defined in the contract, remote support includes access to the system, which must always be authorised and controlled by the Customer/Data Controller. Therefore, each access is recorded by the operator who carries it out by saving the e-mail exchange.

CONTRACTORS TO WHOM THE SUPPORT SERVICE IS PROVIDED

The support service is provided to:

- Direct Zucchetti Axess customers

- Indirect customers

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 Ad Hoc;

- for indirect customers, the request is sent directly by the customer to a dedicated mailbox (support@axesstmc.com) and it is used as HDA ticketing tool.

Support is provided on both Xatlas software and hardware (firmware) as well as video surveillance systems (whether integrated within Xatlas or not).

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.

If, during the support activity, Zucchetti Axess appointees need to retrieve archives or databases in order to solve the highlighted problems, they must inform the Customer/Data Controller and formalise, even by simply sending an e-mail, the information that they have retrieved the DB's with the Customer's approval. At the end of the activity at the Zucchetti AX offices, the appointee who managed the intervention will delete the data; should it be necessary to store the data for a further period of time, a specific e-mail will have to be sent to the Customer/Data Controller with the following minimum content:
”Dear Customer, we inform you that the notified problem, which required the collection of your archives, was solved. We would like to inform you that we will store the archives from our information systems for the next X days (to be defined from time to time as the need requires it). At the end of the agreed period, the archives will be removed from Zucchetti Axess information systems and will no longer be restored”.

TELEPHONE SUPPORT

There are no problems as far as the processing of the personal data 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 problem 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 cannot be used in trial mode 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 seen 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 problem notified by you. If you add attachments containing personal data to the reply message, these will be saved in the ticketing tool and/or in the e-mail attachments and stored there for 3 years. 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 be sent the customer's access credentials 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 connection with TeamViewer (or equivalent tool).

Every e-mail must be signed with the first and last name of the operator who handled the Customer's problem and the information must be saved in the ticketing tool and/or in the e-mail.

Clarifications:
The disclaimer can also be added within web tickets.
Personal e-mails should not be used, as they cannot be controlled.

SUPPORT VIA CUSTOMERS' DATABASE IMPORT

If, in order to solve the problem 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 problem notified by you, it is necessary to perform verifications on 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 problem and will be deleted by Zucchetti Axess appointees at the end of the intervention.
Data must be saved in the Directory not 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 problems on the archives that you sent, we request the authorisation to store your archives on our infrastructure for the following ______ days. The purpose of this storage is to check for possible problems that you may notify during the use of the restored archives. At the end of the above-mentioned period, we will proceed to the permanent archive removal. 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 problem notified 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 TEAMVIEWER 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 offers 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 TeamViewer, it is possible to also provide 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.

If there are codes, passwords or licenses that we must add for the proper operation of the tool and which the customer is not meant to see, it is essential to use the TeamViewer function: Show black screen

It is essential to use our TeamViewer as it is licensed and customised with all the documentation required by law for personal data processing.
Only in exceptional cases and after a careful assessment performed by the manager and by the privacy office, it is possible to use other connection tools that operate in the same way.

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.

It is necessary to send an e-mail to the customer:
“For the execution of the support activities requested by you, it is necessary to create individual access profiles for the operators who will perform those activities. To this end, it is necessary to generate those access credentials to the system.”

When the customer makes the request after the individual user name has been created:

“For the execution of the support activity requested by you, you need to enable the user name matched to me”

At the end:
“The support activity is completed. We remind you to disable the credentials in order to protect your personal data”.

OTHER TYPES OF SUPPORT

The support is also performed on video surveillance systems. When the video camera does not work, if the system is integrated within Xatlas, you intervene directly in Xatlas; in these cases, access is made to the configuration settings or images but only in real time and nobody ever accesses the records. If the records are not valid, support is given to the video surveillance system maintenance technicians.