Author	Privacy Office/Product Manager
Approval	Alberto Pavesi

Revision version

Version	Author	Consultation of DPO	Issuance date	Reason for the revision
0.0	Privacy Office/Product Manager	24/05/2018	25/05/2018	First release
1.0	Privacy Office/Product Manager	18/06/2019	19/06/2019	Added logo; added versioning; the purpose of the processing has been changed
2.0	Privacy Office/Product Manager		26/11/2020	Support procedures added, approver changed
3.0	Privacy Office/Product Manager	05/11/2021	12/11/2021	Specific functionalities added for the validation of the Green Pass with reference to X3 and QRBOX products
4.0	Privacy Office/Product Manager	30/11/2021	01/12/2021	The following products have been added: • 934 i-door+ / i-door • 968 SuperGLASS 7 TRACK • 966/964/962 SuperTRAX TRACK • Tornelli: 892 TRAXGATE - 893 X1GATE – 891 MAXGATE • 921 XA4 / XA4K • 907 MINIBIOX
5.0	Privacy Office/Product Manager	13/01/2022		The following products have been added: XFACE M/XFACE 7/ AccessC19
6.0	Privacy Office/Product Manager	21/03/2024	21/03/2024	Updated list of products: • 937 X7 GLASS added; • App Access C19 removed

OPINION OF DPO

OK.

ZUCCHETTI SERVICES AND PRODUCTS RELATED TO GDPR PROVISIONS:
Access controls with badge or biometry: 934 XIO / i-door+ / i-door - 933 AX GATE - 932 AX DOOR -
968 SuperGLASS 7 Light and TRACK – 966 / 964 / 962 SuperTRAX Light and TRACK / 906 XFace M / 972 XFace 7
Turnstiles with integrated terminal or controller: 892 TRAXGATE - 893 X1GATE – 891 MAXGATE
937 X7 GLASS / X7 - 967 X4 GLASS / X4 - 921 XA4 / XA4K - 931 X3 / X3BIO - 930 X1 / X2 / X2BIO
Read and write biometric data: 905 FingerBox and FingerBox+ - 906 XFinger –
907 AX BIO / MINIBIOX

DATA PROCESSOR					
Name	Zucchetti Axess S.p.a.				
VAT no.	03537610960				
Address	Via Solferino,1				
Città	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
The indicated terminals are used to recognise individuals by means of badges or digital fingerprints in order to carry out an access control. • X3+QRBOX / X3BIO+QRBOX/X4+QRBOX / X7+QRBOX With specific reference to X3 and QRBOX terminals, it is possible to activate the Green Pass recognition and verification function. The read QR CODE is not transmitted outside the terminal, it is used locally for verification purposes only and is neither stored nor transmitted. No health data is displayed or accessible unless the QR CODE is temporarily used to authorise access to the gate.

- **XFace M (906.908.8x) - XFace 7 (972.172.xx)**

XFace M and XFace 7 are readers with face recognition capabilities.
If a face is recognised, only the numeric code identifying the recognised user is sent to the terminal connected to the reader, in encrypted and proprietary format.

XFace M is also fitted with a thermoscanner for checking body temperature.
The data is not stored but only used to check whether it is above or below a settable threshold.

XFace M can also check the Green Pass if it is equipped with an optional QR reader.
Checking the Green Pass is based on an SDK certified by Sogei (verificac19-sdk-php) and available on github (https://github.com/herald-si/verificac19-sdk-php).
The terminal updates certificates and rules by connecting to the national server as required by regulations.
The result of the green pass validation, together with the name and surname of the pass holder, is communicated using a proprietary encrypted protocol to a terminal usually installed in conjunction with the XFace M.

PURPOSE OF THE PROCESSING

The purpose of the terminals is to enable the access control within the company and to manage security.
The purpose of the processing of the Data Processor is to provide support and maintenance services to the Data Controller.

CATEGORY OF INTERESTED PERSONS

Employees and co-workers, visitors.

PERSONAL DATA CATEGORIES

Personal Data: identification data, accesses of the persons to the gates.
Special categories of personal data: Biometric data (digital fingerprint).

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.

TERMINAL SERIES: 934 XIO / i-door+ / i-door - 933 AX GATE - 932 AX DOOR - 968 SuperGLASS 7 Light - 966 / 964 / 962 SuperTRAX Light - 937 X7 - 967 X4 GLASS / X4 - 921 XA4 / XA4K - 931 X3 / X3BIO - 930 X1 / X2 / X2BIO - 892 TRAXGATE - 893 X1GATE – 891 MAXGATE

The terminals in question (*as of firmware version G01 onwards*) have the following features to protect the personal data they process:

- Encryption of files containing personal data
- Registered user names for administrators
- Password protection for administrators

- Secure HTTPS communications (*)
- HASH keys to avoid fraudulent tampering with timestamp records

(*) Not available for the 930 X1 / X2 /X2BIO family, on the 893 X1GATE, 891 MAXGATE turnstiles and on the 933 AX GATE and 932 AX DOOR controllers. However, data exchanged using a non-secure protocol (HTTP) may be sent in encrypted format.

TERMINAL SERIES: 968 SuperGLASS 7 TRACK – 966 / 964 / 962 SuperTRAX TRACK. The data stored in the internal memory, in order to be understandable, must only be downloaded with software based on proprietary DLLs provided free of charge by AXESS TMC.

TERMINAL SERIES: 905 FingerBox and FingerBox+ - 906 XFinger – 907 AX BIO / MINIBIOX - 931 X3BIO - 930 X2BIO

Zucchetti Axess S.p.A. informs you that your personal data are protected by the following mechanisms:

- Only "**digital fingerprint templates**" are stored (hereinafter: "templates"). Digital fingerprint images will not be stored. The **templates** are binary data containing only geometric features of the fingerprints:
  - The templates are created with proprietary algorithm and the template structure is confidential information that is not disclosed to individuals or companies.
  - It is impossible to reconstruct digital fingerprint images from templates. The size of a single template is about 400 bytes while the fingerprint image should be a few tens of kilobytes.
  - The raw biometric data or the image of the fingerprint, generated during the biometric acquisition process, are never saved in memory areas, not even temporary, be it central or secondary, nor are they written on the filesystem of the system used for the acquisition.
  - The biometric data is never made available as an output from the sensor to reduce the risk of fraudulent acquisition with third-in-the-middle attacks on the sensor or its communication channels with the biometric system.
  - The Data Controller only stores templates not digital fingerprint images

- To further increase security, all files used to exchange templates between biometric devices can be in an encrypted format
- In our product range, there is also a sensor version that can detect the "vitality" of the biometric feature ("live finger")
- Zucchetti Axess biometric terminals can also store the template on a badge owned by the user and verify it by comparison (**verification**). In this mode, the fingerprint "templates" are stored on a "**RF smart card**" with a memory of 4 KB (hereafter also referred to as "**badge**") owned by the user. In the "**Verification**" mode **with fingerprint on badge**, the templates are not permanently stored on Zucchetti Axess devices. In this mode:
  - the conscious cooperation of the person concerned is required as the badge is in his/her exclusive possession. The presence of the user can be detected if s/he approaches the badge to the reader
  - During the enrolment phase (creation and acquisition of a new template of the user's fingerprint), the biometric template is temporarily stored only for the technical time of writing on the user's card which occurs in less than one second. The template is immediately deleted from the terminal memory once it is saved on the user's badge. The template remains stored only on the user's smart card.
  - The verification/access phase starts when the user approaches his/her badge to the terminal reader. During the access phase, the fingerprint template is read by the badge and temporarily stored on the terminal memory (not accessible from the outside). The template is destroyed after the verification of the fingerprint or at least after a timeout of a few seconds.
  - The biometric templates are processed only during the registration (enrolment) and access (verification) phases. They are exchanged between the user card and the internal memory where they are temporarily stored. Templates are never transferred to an external system.

- Biometric templates are only stored on the badge for the exclusive use of the user in encrypted format with triple DES algorithm. The template can also be stored in a password-protected memory area of the badge.
- It is not possible, under any circumstance, to reconstruct the digital fingerprint image from the data saved on the badge (the template). Even if someone managed to extract the template from the badge, they could not reconstruct the image of the fingerprint.
- The badges are only readable by Zucchetti Axess biometric devices.
- The biometric template is not readable by system administrators as it does not reside on the terminal itself, but only on the user's badge.

<u>TERMINAL SERIES</u>: XFace M (906.908.8x) - XFace 7 (972.172.xx)

Zucchetti Axess S.p.A. informs you that your personal data is protected by the following mechanisms:

- Users' JPG photos are stored on the internal memory of the terminal together with the biometric template extracted from the photos. The biometric template is stored in encrypted mode and the templates, even if decrypted, are not reversible.

  Moreover, they cannot be loaded and used on another facial terminal even of the same type, as each terminal has a system code and the templates can only work on terminals with the same system code.

  The system code is only known to the administrator and it is stored in encrypted format in the terminal

- Administrators can access the reader via SSH and via HTTPS and have access to users' JPG photos
- The login is encrypted, passwords are stored in encrypted format. The system code, once changed, is no longer visible, not even to the administrator.
- The photos of users' faces can be uploaded on the internal memory of the reader via encrypted transmission, or they can be captured using the built-in camera of the reader and stored on the internal memory avoiding transmission over the network.

The features must be enabled by the Data Controller.

1. 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.