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

Revision version

Version	Author	Consultation of DPO	Issuance date	Reason for the revision
0.0	Ufficio Privacy (Zucchetti Spa)/Development Manager	05/11/2021	12/11/2021	First release

OPINION OF DPO
OK.

ENTRO APP

DATA PROCESSOR

Denominazione	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

Entro is the mobile application of Axess TMC, available both for iOS and for Android, it allows timestamping the timecard, opening doors, turnstiles and gates by means of a smartphone, using Axess TMC terminals fitted with BLE (Bluetooth Low Energy) readers.
In addition to employees, **Entro** can also be used by visitors for independent access without passing through a reception desk.
All terminals and controllers from the Axess offer can be fitted with a BLE reader, provided with a TTL serial interface, thus allowing the user to identify himself/herself by means of a smartphone.

When installed on a smartphone, the **Entro** app automatically generates a unique code that will be sent to terminals to identify the user in exactly the same way as a badge code. The user can see this numeric code, can copy it, paste it and send it to the information system managers to have it entered on the white list in the same way as a badge code.

Each time it is launched, the **Entro** app shows the user a list of available BLE readers within a 10-metre radius (if there is more than one). The user chooses on which reader to identify himself/herself. It is also possible to configure the app to automatically send the user code to the first available reader.

PURPOSE OF THE PROCESSING

Using the App for timestamping the timecard and for overcoming the access control.
The purpose of the processing is to provide assistance and maintenance services to the Data Controller.

CATEGORY OF INTERESTED PERSONS

Employees and co-workers, visitors.

PERSONAL DATA CATEGORIES

A distinction is made between two cases depending on whether the **Entro** APP is used in conjunction with the Entry365 service or not.

- Use without registering to the Entry365 cloud service
In this scenario, no data is requested from the user.
The only data that can be associated with the user in the access control software is the unique code that is generated by the Entro App upon installation and which the Entro App transmits in BLE to the terminals as if it were the badge code. If the user changes smartphones, s/he must reinstall the Entro app, which will generate a different code.
There is no way to keep the same code. If the user uninstalls the Entro app, the code is deleted.

- *Use by registering to the Entry365 cloud service.*

By means of the Entro app, it is possible to register to the Entry365 cloud service. In this case, the user must enter the e-mail address, the name and the surname. These data will be sent (by means of a cellular network with secure protocol) to the Entry365 cloud server and will also be stored in the Entro app data on the phone.
In this scenario, the unique code which will be used to identify the user is generated by Entry365 and sent to the smartphone. The ENTRO APP stores it.
The companies acquire the identification number of the user by means of the Entry365 service. The user is no longer required to copy the code and send it to be entered on the white list.
If the user changes the smartphone, s/he keeps the same code: reinstalls the Entro app which will receive from Entry365 the identification code associated with the user's e-mail.
In this scenario, a proper button is available to delete the data stored on the user's smartphone and disconnect it from the Entry365 service.

Note: for information on the data processing performed by Entry365, please refer to the specific processing register

CATEGORY OF RECIPIENTS TO WHOM THE DATA CAN BE COMMUNICATED

Other companies of Zucchetti Group
Subcontractors

DATA TRANSFER ABROAD

The data transfer abroad is not provided by the Data Processor.

RETENTION TIME

Again, a distinction is made between the two scenarios, i.e. whether the **Entro** app is used in conjunction with the Entry365 service or not.

- Use without registering to the Entry365 cloud service

In this scenario, the only data stored on the smartphone is the unique code generated by **Entro** upon installation. This data is deleted when you uninstall the Entro app.

- *Use by registering to the Entry365 cloud service.*

If the user has registered to the Entry365 service, then, in addition to the user identification code received from Entry365, the user's e-mail, first name and last name are also stored within the ENTRO app. The data is stored within ENTRO until the user presses the "disconnect the device" button from Entry365. In this case, the data is deleted from the phone and the identification code received from Entry365 is replaced with a unique code generated by the app itself.

Note: for information on the data processing performed by Entry365, please refer to the specific processing register

1. TECHNICAL MEASURES THAT CAN BE IMPLEMENTED IN THE APP

The Entro app benefits from all the security measures that the user can decide to activate directly on his/her smartphone, such as facial recognition, fingerprinting, access code, etc.

With specific reference to the Entro App, the security measures are hereinafter presented:

- The unique code (and possibly first name, last name and e-mail in the case of registration to the Entry365 service) is stored on the device in encrypted format;
- The identification code is sent via Bluetooth (BLE) to the access control terminal, in encrypted format

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.