Author	Privacy Office Zucchetti S.p.a.
Approval	Marco Marchetti

Revision version

Version	Author	Date	Reason for the revision
0.0	Privacy Office Zucchetti S.p.a.	07/12/2018	First release
1.0	Privacy Office Zucchetti S.p.a.	25/09/2019	Versioning added; the purpose of the processing has changed; the data deletion terms for the Cloud services have been specified.
2.0	Privacy Office Zucchetti S.p.a.	11/02/2020	Change of the Cloud service supplier

OPINION OF DPO OK.

OLTRE

DATA PROCESSOR

Name	ZUCCHETTI AXESS SPA				
VAT no.	03537610960				
Address	VIA SOLFERINO 1				
City	LODI	Postal code	26900	Prov.	LO
Legal representative	DOMENICO UGGERI				

ORGANISATIONAL STRUCTURE

Division	AXESS	Division Manager	MARCO MARCHETTI
Area	OLTREMARE	AREA MANAGER	ROBERTO FIDEL

PERSON IN CHARGE OF PROCESSING

DEVELOPMENT
COMMERCIAL
AFTER SALE
HELP DESK

CONTACT DATA

Data Controller	Zucchetti Axess S.p.a.	Ufficio.privacy@zucchetti.it	+39 037.15941
Representative of Data Controller	N/A		
Data Protection Officer (DPO)	Mario Brocca	dpo@zucchetti.it	+39 0371. 5943191

DESCRIPTION

The OLTRE suite is composed of a portal which manages customer services by means of various integrated modules managing the following processes: time and attendance management, shift management, access management, collection of start and end data of the production activity, collection of data from fixed and mobile terminals, guard patrol management.

ARUBA.php: it is the application for time and attendance of the company personnel which, even with a proper app installed on the mobile device (OLTRE.app), allows the employee to activate the work attendance process. With the app, the geolocation is activated as well, which can be controlled by the user who can activate it or deactivate it. It is the customer who has acquired the services to configure the system in order to have or not the geolocation data in the database tables.

The application can also manage biometric data, if the customer choses to install biometric terminals. In this case, the alphanumeric string corresponding to the digital fingerprint is saved in a database table so that the data can be distributed to all terminals.

ARBE.php: it is the application that allows managing the work shifts.
ELBA.php: it is the application that manages the control of physical accesses and that allows identifying the geolocation of terminals in order to check their spatial location. In this case as well, geolocation coordinates are saved, but they only refer to the machine, and not to persons.
ANTIOPE.php: it is the application used by the company to record the activities carried out on the production machines (or on a bench). The operator enters the activity start/suspension/end times in order to register all performed activities and the processing times;
ANTIGUA.php: it is the application that allows exchanging data with terminals and mobile devices. Personal data are not processed, if the app is limited to the collection of transactions without associating them to a person, if however, an archive of persons with the relative badge number is managed, personal data will be processed (the choice is optional upon the order).
CATALINA.php: it is the application that allows managing the guard patrols of operators in charge with physical safety and that allows registering that all places provided by the contract with the customer have been visited.
The project also includes other applications: for queue management and meal booking.
PANAREA.php: it is the application that allows managing, anonymously as well, the queues at the public and private services. Personal data are not processed, if the application is limited to withdrawing an access order number, if instead queues which provide a booking are managed, personal data will be processed (the choice is optional upon the order).
PASTI.biz: it is the application which allows booking meals in hospitals, schools, companies. The persons can select the menu from the available ones, in order to send the bookings to the supplier for meal preparation.

PURPOSE OF THE PROCESSING

OLTRE suite is an integrated system which puts at disposal software applications with the purpose of simplifying company processes. Il allows recording the attendance, accesses, work shifts, working activity performance times and managing the hardware infrastructure necessary and preparatory for the described purposes.
Certain applications, with special setups, do not manage personal data (ANTIGUA.php, PANAREA.php).
The application for meal booking has been designed to optimise the meal preparation times and to allow meal preparation according to the assigned diet and, if the case, to the preference.
All these features are managed by only one system. All data from common databases and, therefore, application securities are common to all services.
The purpose of the processing is to provide assistance and maintenance services to the Data Controller.

CATEGORY OF INTERESTED PERSONS

OLTRE suite is aimed for companies: data of employees, collaborators, visitors and guests can be managed and processed.

PERSONAL DATA CATEGORIES

Personal data for most biographical information. Depending on the provided service, data can be related to the attendance of personnel, to the activities carried out by the personnel and to the work shift management. In all these cases, personal data are processed.
Data with specific risks: biometric data; geolocation coordinates; data related to meals/diets.

CATEGORY OF RECIPIENTS TO WHOM THE DATA CAN BE COMMUNICATED

Only for Cloud version, data are communicated to AWS, manager of Data Centre and the related services.

DATA TRANSFER OUTSIDE THE EU

No.

TERMS FOR DATA DELETION

For Cloud services, the data is saved in a file, which is kept for 40 days, while once the data is transferred to the database, it is automatically kept for 3 years and then deleted; the customer can however manually anticipate the deletion.

Instead, in the On-premises version, in absence of automatisms, the choice of data storage duration falls on the customer.

If a customer terminates the contract, data are stored for the next 30 days and then deleted from the production environment. Backup data is stored, only for storage purposes, for the next 12 months.

GENERAL DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SAFETY MEASURES

1. EXISTING SAFETY MEASURES

Transactions arrive on the server via http or https protocol, depending on the terminal used by the customer and the configuration made.

The OLTRE app communicates by default via https protocol, however, it is possible to configure it in http (for the On Premise version).

When the service is activated, a superuser account is delivered to the customer with which new authorisation profiles can be created. Authorisation profiles can be generated both for a single function and in relation to the events that can be generated on the database records (edit, add, delete, view, print, process, etc.). It is not possible to have several users with the same name.

The following password options can be configured for each user:

- Complexity (lower case/upper case, numbers, special characters)
- Length (8-32 characters)
- Validity (from one day to 6 months)
- Number of previous passwords that cannot be reused
- Mandatory change or not at first login.

The passwords are encrypted in the database with SHA256

The users will be automatically disabled after 6 months of inactivity.

On the database, there is a log with all change operations operated within the system. The logs are stored for 40 days (this value can be set for the On-premises versions). The logs can be displayed by authorisation level.

It is possible to delete data related to a person, as well as to export it to csv format.

It is possible to delete a customer's data together with all data related to him/her, as well as to export them to csv format.

It is possible to archive in text format and/or delete all “dynamic” data (e.g.: attendance transactions, access transactions, timecard data) of only one customer. The function is also available for non-supervisor users, if enabled.

On the principle of minimisation, data are automatically stored for 3 years for the Cloud version (the duration cannot be customised by customer). For the On-premises version, which is not fitted with this automatism, the customer chooses, who has the possibility to store and/or remove data with standard application functions.

Everything existing in the database can be extracted. Every extraction and printing can be made with a “creator pdf”; personal data can be extracted to xml.

The possibility is provided to create the encryption for data related to:

- Geolocation coordinates: the Data Controller may limit the number of decimal places in the coordinates themselves, thus degrading the accuracy of the actual position
- For newer terminals that allow it, it is possible to enable encryption of sent transactions.

2. SAFETY MEASURES TO IMPLEMENT

Create the encryption for data related to:

- Biometric data: they must all be encrypted, above all, if a system is used with biometric data on HW and not on the card of the person concerned
- Data related to patient's diet: check the table fields in which the encryption can be implemented so that customers that register the disease based on which the diet is provided are protected against unauthorised accesses to such information.
- Create the encryption for passing/communicating data between the systems: for example, as regards the sent tables;

Provide the possibility to cloud customers as well to choose the data storage time. Today a 3 year period is valid for everybody, but, according to the demands, different requests can exist.

3. SAFETY MEASURES FOR SUPPORT ACTIVITIES

The support service for OLTRE suite products and services is provided to:

- Direct customers
- Partners contracted as customers
- Customers whose support is subcontracted to partners

The support, depending on the supply method, is performed in various ways.

On-site support

The operators access the customer's structure in order to perform a training or a technical maintenance activity.

In this case, they work as if they were part of the customer's structure and they implement all the procedures required by the customer. The customers can generate individual users for accessing their systems or they can access alongside in order to train their staff.

If, during the support activity, the archives or databases must be collected for solving the reported issues, it is necessary to inform the customer and to fill in the Intervention note:

- Collected archive
- The purposes for which the archive has been collected
- The customer's representative who authorised the collection of the archive

Once the reported issue is solved, the customer will be notified on the adopted solution and on the upcoming archive deletion.

The minimum content of the e-mail is the following:

”Dear Customer, we inform you that the reported issue, which required the collection of your archives, was solved. We inform you that we have removed the archives from our information systems and destroyed the possibly produced hard copy documents.”

If you need to store the archives for the necessary time to test the adopted solution:

”Dear Customer, we inform you that the reported issue, which required the collection of your archives, was solved. We hereby notify you that we will store the archives in our information systems for the next 7 days. At the end of the agreed period, the archives will be removed and will no longer be restored”.

The same procedure must be followed if an archive is collected, sent to the support and the issue is solved during the intervention at the customer, therefore without being necessary to examine it once returned on the premises.

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.

It is necessary to pay attention if the customer informs you that the phone call will be recorded. If there is a registration notification, it is necessary to note this event in the used CRM indicating the customers' structure representatives, who can be contacted for exercising Zucchetti Axess rights.

If Zucchetti Axess records the phone calls, the customer must be notified and s/he must be provided with information on the representatives whom can be contacted for exercising his/her rights. The reference for this purpose must be ufficio.privacy@zucchetti.it. In this case as well, the event will be mentioned in CRM.

E-mail support

In case of e-mail support, 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 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”.

Any access credentials of the customer received by e-mail will be discarded, will not be stored and will be deleted (the ones of the customer, not those generated properly for the technicians performing the support and which can also be received by e-mail): if a customer/partner sends access credentials to his/her environment without the request of Zucchetti Axess, s/he will be replied that Zucchetti Axess is not authorised to access the systems with credentials of other users as this method infringes the EU Regulation 2016/679 (GDPR). Therefore, individual credentials or a connection with remote desktop tools (for commercial use) will be requested.

Every e-mail will be signed with the name and surname of the operator who handled the customer's issue and the information will be stored in CRM (only the name is enough, or the nickname Zucchetti Axess).

Support via customers' database import

If, in order to solve the issue reported by the customer, it is necessary to send databases or other files containing personal data, the download of the archives will be made via WeTransfer or via a connection link on the customers' environments: in this case, the management is performed by the customer who provides the credentials to access the environment where the archives are located. The support must download them on network disks, which are not subject to backup, and delete them when the activity is completed.

Support generated by the necessity of having the backup of the customers of a Cloud service

The written or verbal authorisation proof of the customer must exist in CRM.

The system analysts will not be able to extract any backup from the customers for other requirements and purposes than to provide support to the customers; for instance, they are not allowed to perform backups used for the production of a test execution.

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 accesses an environment with an authorisation profile chosen by him/her in order to perform the support activities
- The customer can disconnect whenever s/he wishes

It is essential to use a licensed tool for commercial use and customized with the entire documentation required by the law on 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 through remote connection on public IPs or via VPN

If the support activity must be performed on cloud systems on public IPs or via VPN or private accesses, the operators must access 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

The rules regarding customers' environments, regardless of the delivery form (SaaS/PaaS/On-premises) are the following:

- creation of users for application consultants:

In order to perform all the start-up activities in the customer's environment, a user must be properly created within the system (who will have the user profile "Zucchetti Axess User") with this "login name": ZA_+ the first 3 letters of the surname + the first 3 letters of the name.

This way, the Customer can acknowledge the source of the user (e.g. for Rossi Mario Subject, the following user should be created: ZA_ROSMAR).

The customer must be involved in the creation and s/he must be guided in the access and user creation process, specifying and sharing with him/her the assigned rights (definition of user profile).

- creation of users for the support staff:

To the support request, an e-mail will be sent to the customer, specifying the information necessary for the creation of the "login name" who will perform the support. The creation rules already explained for application consultants will apply.

At the end of the support, an e-mail will be sent to the customer:

"The support activity is completed. We remind you to disable the credentials in order to protect your personal data".

Start up projects and conversions

Two different situations can exist:

- Conversion or start up with contract

- Conversion or start up without contract

In the first case, the activity is designed to comply with the contractual obligation and it is therefore legal.

In this case, it is necessary to create a project document, in which to agree with the customer on the operational procedures for the execution of the activity, such as:

- Personal data, archives, databases necessary for carrying out the activity
- Detail of the operations that will be performed on the data
- Identification of the period within which such activities will be completed
- A test estimate during which the customer will test the result of the performed work

The documents signed by the customer for carrying out these activities represent the contract and the appointment as processor, giving Zucchetti Axess the right to perform all the necessary activities for the service supply.

In this case, the letter of appointment will not be sent to the customer, as this will be managed by Zucchetti Axess, as supervisor of Zucchetti Axess operators.

Instead, if there is no contract, it is necessary to send the customer the appointment as Data processor.

The carrying out period and the deadline of the activity must be stipulated in the appointment. As Data Processor, Zucchetti Axess will designate the operators.

In this case as well, it is necessary to provide a project phase in which the above-mentioned steps are shared.

At the end, the test must also be provided.

In the test document, which must be signed by the customer, s/he will declare that the performed activities are correct and therefore s/he will authorise us to delete his/her archives.

The test document must contain the following indications:

- The performed service complies with the agreed contractual frame
- The customer has tested the product and declares that it works and that all the functions have been correctly configured and implemented
- That there are no errors in the converted data and therefore that s/he will be able to use the product for the purpose for which it was purchased

Furthermore, the customer must declare that as of the date of signing the contract, s/he will have no claims on the performed conversion activity stipulated in the contract and that s/he authorises Zucchetti Axess to delete every data, archive or database that have been used for carrying out the conversion phase.

Only if it is necessary to store the customer's archives for purposes of caution and verification of the performed work, a notice will be sent to the customer authorising Zucchetti Axess to store the archives for a subsequent period of time, at the end of which the archives must be deleted.

The entire authorisation procedure must be included in the after-sale service in order to keep a history of it in case of need.

All printed documents containing customer data must not be recycled and must be destroyed immediately.

4. SAFETY MEASURES IMPLEMENTED FOR - CLOUD - SERVICES PROVIDED BY AMAZON WEB SERVICES

The safety measures adopted by the cloud service supplier can be referred to by accessing the following link: https://www.amazon.it/gp/help/customer/display.html?nodeId=201908990

The supplier has been appointed as data processor by means of a proper appointment deed which can be referred by accessing the following link: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

The Data Centre is fitted with protection systems against hostile intrusions (firewall and antivirus devices), which have been properly configured in order to guarantee the safety of the information issued and processed by customers.