Data processing in SAAS and PAAS services

Summary information

Responsible for the treatment					
Denomination	Ars Edizioni Informatiche Srl				
Vat	13309950155				
Address	Via Losanna,15				
City	Milan	**Zip**	20154	**Province**	MI
Legal Representative	Giacomo Balestrini				

Persons in charge of processing
Analysis, development, quality control, help desk, application consultants, systems engineers.

Contact details		
Responsible for the treatment	Ars Edizioni Informatiche Srl	privacy@arsedizioni.it 02 3192301

Purpose of the processing

The purpose of the processing is the management of personal data of interested parties, professional studios and companies, aimed at managing personal data in the individual applications and modules used.

Management of documents generated by individual applications through a DMS (Document Management System). The purpose of the processing is to provide assistance and maintenance services to the Customer.

Category concerned

Employees, apprentices, trainees, interns, collaborators, suppliers, contractors, visitors.

Categories of personal data

Personal data of employees, collaborators, contractor suppliers, visitors depending on the application that uses them.

Data relating to the employment relationship with economic data and data relating to the employment contract applied.

Categories of recipients to whom the data may be communicated

Personal data may be communicated to Ars Edizioni Informatiche software design and development personnel, aimed at carrying out assistance and maintenance activities.

Data transfer abroad

NO

Terms for deletion of data

The data stored in the Ars Edizioni Informatiche Data Center will be kept for the entire duration of the contract and for 90 days following its termination. They will be stored on backup media for the next 12 months. The data relating to the administrative and legal management of the contractual relationship will be kept for 10 years from the termination of the contractual relationship.

The Customer has the possibility, through the application functions, to launch massive deletions of personal data saved in the database, only within the duration of the contract.

ARS Edizioni Informatiche declines all responsibility in case of accidental or non-accidental deletion, data breach or other IT or technical incident, regarding the data of Customer who do not have a regular contract in place.

Extensions for data retention are not considered extensions of the contract.

General description of technical and organizational security measures

Security measures implemented in software

The security measures configurable in the application system are:

Manage login credentials

- User name: access to the system takes place only through the unique identification of the person accessing it. In the system there is an administrative credential which is delivered to the holder and can be used by him only in exceptional circumstances. The owner must prepare an organizational procedure so that this user is assigned to a single person in charge and is managed in compliance with good management rules.
- Password: Password complexity rules are not configurable. A highly complex password is always required.
- Deactivation / disabling of credentials: the deactivation of unused credentials or the disabling of credentials of persons in charge who no longer have the subjective characteristics to access that personal data, are configurable in the system by the customer.

- Authorization profiles: the Customer can configure access to personal data processed in the system depending on the activities carried out by users.

Identification of who processed the data

- Log tools: The Customer can request logs of all activities performed on the data, including accesses and modification operations. Logs are enabled by default and cannot be disabled by the Customer.
- Logs can be requested within 45 days.
- The logs are not directly accessible by the Customer.
- Presence of service users for assistance personnel: Those who perform assistance and maintenance on the procedure have nominal users that must be activated and deactivated by the Customer as needed.

Encryption techniques

Encryption techniques

- Password encryption: An encrypted value with AES256 is recorded instead of the plaintext password.
- Database encryption: not available.
- DMS file encryption: all documents generated by applications and stored in the DMS, or attached as an external document, are encrypted with AES256

Privacy by default

- User profile activation: users in the portal are activated according to a logic of not assigning any authorization profile on the processed data. The Customer will independently choose the appropriate user profiling and assign the authorizations according to the homogeneous area to which the user belongs or the individual authorization profile.

Rights of the interested parties

- Rights of the interested parties: to guarantee the right to be forgotten to the interested parties, it is sufficient that they send a request to the Customer who will make the appropriate assessments. If the Customer decides that the data must be deleted, he can act directly, deleting the master data within each application or module; No information will be available, even indirectly, on that interested party with the exception of the name of those who performed a past activity on a data still in use (historical).

Data processor: security measures implemented for support services

Ticket/email support

The Ars Edizioni Informatiche employee is not authorized to have the Customer's access credentials sent by e-mail nor can he save them on the support and ticketing tool.

If a Customer sends his access credentials without request from the Ars Edizioni Informatiche technician, it is necessary that the same responds that he is not authorized to access the systems with credentials of other users as this mode violates the GDPR. Therefore, the Ars Edizioni Informatiche technician must request the activation of the generic support user that can be activated/deactivated by the Customer.

The support user is always and only support@arsedizioni.it and is activated by default. If the Customer does not wish it, he must disable it.

Use of data in the Customer's database

The Ars Edizioni Informatiche employee who provides assistance to the Customer is authorized to access the customer's data for:

a) Verify unexpected behavior;
b) Correct an error and verify the effectiveness of the solution adopted;
c) Develop customizations

Data processor: security measures implemented for SAAS-PAAS services

Summary

CODE	CLASS	APPLICATION LAYER
M1	Local and equipment security	The technical areas of competence of Ars Edizioni Informatiche are characterized by measures that control physical access to the premises.
M2	Authentication	Ars Edizioni Informatiche systems and services are accessible only by passing an authentication procedure that involves the use of credentials associated with appointees.
M3	Authorisation system	Access to data is controlled through authorization profiles defined at the operating system level of the platform hosting the application (Windows) and at the application level.
M4	Data Integrity Check	Virus control services are active both in the local file systems of individual PCs and in shared file systems, as well as on e-mail messages.
M5	Data Backup and Restore	Backup policies are in place for data. Activities are implemented aimed at reducing the disruption in the event of failure (disaster / recovery)
M6	Security Policy Management	IT policies are prepared for security.
M7	Removable media	Rules are laid down for the management (custody, use and reuse) of removable media in the presence of sensitive data.
M8	Training of appointees	There is a training and refresher plan for Ars Edizioni Informatiche employees.

Detail

CODE	CLASS	APPLICATION LAYER
M1	1.1 Intruder alarm systems	An intrusion warning system is provided. In the event of an intrusion, the alarm system automatically notifies the Ars Edizioni Informatiche representatives.
	1.2 Access control to restricted areas	Access to the CED is allowed only to authorized personnel. The CED is locked and only authorized personnel are in possession of the keys. Access to the CED is registered.
	1.3 Fire prevention	The premises are equipped with automatic smoke detection systems. The technical rooms provide a system for extinguishing fires. The security measures provided for by Legislative Decree 81/2008 are applied.
	1.4 Relocation of active equipment and network servers	All active equipment and network servers are in technical rooms with controlled access.
	1.5 Office access registration	Date and time of entry and exit of clerical staff are recorded with the aid of attendance detection devices.
M2	2.1 Adoption of procedures for managing authentication credentials: USERNAME	All workers are identified in the information system through a username uniquely assigned to them. Access to any environment or electronic tool is through authentication credentials.
	2.2 Adoption of procedures for managing authentication credentials: PASSWORD	Any user who initiates a processing of personal data is informed about the importance that the confidential component of the authentication credential is not disclosed to other operators. In addition, the user is trained on the minimum rules of composition of the password (at least 8 characters and consists of alphanumeric characters not easily attributable to the subject to which they belong). The user is also informed about the need to change passwords every six months if he processes personal data and every three months if he processes sensitive data (judicial data have not been identified in the company to date). The tools used for processing often do not independently manage the password change, nor do they carry out checks on the repetitiveness of the same passwords over time. Therefore, these obligations are the responsibility of the same user.
	2.3 Exclusive use of authentication credentials	Each authentication credential (username and password) is assigned to a single operator who will use it exclusively. It is the customer's responsibility to delete or disable the credentials of an operator who is no longer part of his organization. It is the customer's task and responsibility to ensure the correct application of the rules for the non-disclosure of credentials. ARS Edizioni Informatiche declines any responsibility inherent in the violation through credentials defined and managed entirely by the customer.
M3	3.1 Authorization profile for individual appointees	This process guarantees, upon passing the authentication phase, the correct and complete association between users and objects of the computer system connected to the assigned profile; includes all the information, associated with a person, aimed at identifying which data he can access and also what treatments he can use; It establishes which areas of the IT system the user can access and what actions, once entered, he can perform.

CODE	CLASS	APPLICATION LAYER
M4	4.1 Computer security architecture	There is a set of behavioral rules and operating procedures aimed at protecting the entire computer system. In particular, it provides for the adoption of programs aimed at preventing the vulnerability of electronic instruments, on the one hand by counteracting external attacks, on the other by correcting the defects inherent in the instruments themselves. In relation to the correction of defects, it operates the constant updating of the products and the periodic verification of the installation and configuration of the software products. In relation to the protection from external intrusions on the initiative of the "criminal mind", the antivirus architecture uses IDS (Intrusion Detection System) systems, managed by the Ars Edizioni Informatiche Systems Group, aimed at identifying any attempt to operate and / or illicitly enter the network and systems placed under protection. An antivirus system is active that monitors the entire corporate network. The system is active on both desktops and laptops. The antivirus is updated every time the manufacturer updates the list of virus reports. The technical office, if it believes that following a request from an operator, the system may be infected, launches the scan to check for any infections. Laptops are equipped with an antivirus system that updates itself every time the laptop connects to the corporate network. There is a firewall system that filters incoming and outgoing communications.
M5	5.1 Backup procedures	Organizational and technical instructions are given to provide for the daily saving of data.
	5.2 Recovery procedures	Appropriate measures shall be taken to ensure that access to the data is restored in the event of data being damaged and shall not exceed seven days. Activities are also planned to reduce the disruption in the event of a breakdown.
M6	6.1 Policy for the use of IT tools	Policies are prepared for the use of electronic tools relating to: -Use of the PC -Internet browsing -Use of e-mail
M7	7.1 Instructions to appointees	Organizational and technical instructions are given for the custody and use of removable media on which the data are stored in order to avoid unauthorized access and unauthorized processing.
	7.2 Storage, use and reuse of removable media	Removable media containing sensitive or judicial data, if not used, are destroyed or rendered unusable, or can be reused by other persons in charge, not authorized to process the same data, if the information previously contained therein is not intelligible and technically in any way accessible.
M8	8.1 Training Plan for appointees	Training is provided for all Ars Edizioni Informatiche employees.

Data processor: security measures applied to the data center

- *Certifications*: Ars Edizioni Informatiche considers safety a priority and indispensable element for the company and its customers, which is why it has organized its management systems in order to follow strict safety criteria. The organization of a management system requires the creation of roles, flows of activities and clearly defined procedures to oversee business processes. Certifications: ISO 27001.
- *Compliance*: Ars Edizioni Informatiche's business processes comply with current regulations, in particular regarding compliance with privacy requirements. In this context, the company has adapted its management system to the requests of the provision of the Guarantor for the Protection of Personal Data regarding system administrators. If the legal requirements are modified, Ars Edizioni Informatiche will immediately adapt the methods of providing the service and the technical characteristics to comply with any changes.
- *Access to information*: the Ars Edizioni Informatiche management system explicitly classifies the level of confidentiality of each document. In particular, documents containing information on security systems are classified as confidential and are not disseminated outside the company.
- *Access to systems: accesses* to systems can always be classified into production accesses and administration accesses. Production accesses are those objects of the provision of the service. Administration accesses are those made by Ars Edizioni Informatiche or by the customer for different purposes such as maintenance, verification of anomalies, data acquisition. Administration access by Ars Edizioni Informatiche is reserved for personnel with the qualification ("role") of system administrator. The company pays particular attention to the assignment of this role only to personnel of high technical skills and having characteristics of proven reliability and morality. Administrative access to systems by customer personnel will be through the nominal assignment of personnel to roles to which access privileges are assigned.
- *System security*: security services are considered active and functioning to protect the components hosted in the Datacenter. Protection systems are designed to maximize protection and are administered by specially trained personnel who follow stringent operating procedures.
- *Security checks*: Penetration Tests and Vulnerability Assessments are carried out annually on the entire Datacenter infrastructure
- *Firewalling*: Datacenter networking is separated from public networks, other Ars Edizioni Informatiche networks and other customer networks. Data flows between the datacenter

networking and the outside are mediated by firewall systems. These firewall systems allow transit only to data flows necessary for the operation of the service and explicitly authorized.

- *Intrusion Prevention*: the Datacenter is protected by Intrusion Prevention System (IPS) systems that allow you to analyze all incoming traffic by immediately identifying attack attempts in progress. Network traffic, on significant segments of the platform, passes through systems that inspect every packet of transit traffic and behave transparently towards legitimate traffic.
- *Antivirus Filesystem*: all servers have Antivirus modules on the filesystem and, on a design basis, specific antivirus products can be configured centrally managed in terms of updating, policy distribution, on-demand scanning, notifications and quarantine area management.
- *Security Patch Management: the* platform is subject to a periodic verification process of patches or fixes released by the manufacturer and considered critical for the provision of the service or for security. The application of the patches will be subject to prior communication to the customer and the scheduling will take place in agreement with the latter.
- *Continuity and emergency*: the Datacenter have been designed to provide maximum reliability in terms of server power supply, as each rack is connected to two independent power supplies (electrical panels attested on redundant UPS), to allow the maintenance of the individual power lines without creating disservice and to avoid blackouts in the event of a fault of a power line.
- *Communication lines*: the solutions and services offered can be provided via secure Internet connection (https). The customer can choose to set up a VPN or MPLS communication line at his own expense.