PRIVACY POLICY

Our GDPR Compliance Statement

Welcome to TESISQUARE®

CONNECTING PEOPLE, TECHNOLOGY,
AND PROCESSES IN A COLLABORATION SQUARE

Review and approval

ACTION	NAME	DEPT.	DATE
Approved	Marco Cuniberti	DPO	21/03/2024
Verified	Alessandro Cassinelli	Legal Manager	21/03/2024
Written	Francesca Bordino	Privacy Specialist	21/03/2024

Distribution

Dept.	
Everyone	Everyone

Update

VER	AUTHOR	DATE	NOTE
1.0	Francesca Bordino	21/03/2024	First draft
2.0	Francesca Bordino	20/06/2024	Creation paragraph Policy on extra-EU data transfer

Index

1 Introduction

The General Data Protection Regulation (GDPR), which entered into force in the countries of the European Union on May 25, 2018, establishes rules relating to the protection of natural persons with regard to the processing of personal data, as well as rules relating to the free movement of such data. It also protects the fundamental rights and freedoms of natural persons, in particular the right to protection of personal data (Article 1 EU Regulation 2016/679).

The Regulation applies to all companies established in the countries of the European Union, and this even if the data subjects are located outside the Union.

The European Regulation does not define the requirements in an analytical and predefined manner, leaving companies with wide autonomy in implementing their compliance programs.

2 Our Commitment

TESISQUARE is committed to ensuring the applicability of the EU Regulation 2016/679, in the forms and ways defined by the company. To this end, TESISQUARE puts in place useful data protection tools and measures to ensure maximum and continuous compliance with the GDPR.

3 Organizational measures to ensure GDPR compliance

TESISQUARE adopts internal organizational measures necessary for compliance with the current regulatory provisions on the protection and safeguarding of personal data. The measures below are taken by the organization in compliance with the general principles of data protection (transparency, purpose, minimization of data, time limitation of the duration of processing, preservation of data integrity).

Periodic training of authorized persons
TESISQUARE activates video training courses on GDPR activated for employees authorized to process personal data in e-learning mode and in-depth privacy courses targeted for specific company tasks.

Privacy organization chart
In order to achieve the organization's internal privacy objectives, TESISQUARE has an organizational chart of functions, defined by assigning well-defined tasks and related responsibilities to all the figures, both internal and external to the organization, who contribute to developing the business processes in which personal data are managed.

Appointment of internal contact persons

TESISQUARE designates the coordinating contact persons in terms of privacy and data protection in compliance with the principle of accountability of the Controller and related duties. Limited to the areas of processing identified for each internal contact person, TESISQUARE recognizes that the designated contact person has the power to sign on his or her behalf the letters of appointment of the External Data Processor should he or she deem it necessary with respect to the Client/Processor. In addition, the person designated through the act of appointment, has the duty to perform all that is necessary to comply with the current regulatory provisions on the protection and safeguarding of personal data.

Letters of assignment to each employee in relation to the task performed
TESISQUARE proceeds with the designation of individuals authorized to process personal data in accordance with the European Regulation 2016/679 and related tasks. In particular, employees are authorized - and given the necessary instructions - for personal data processing activities, as recorded in the Processing Register.

Appointment and verification of the work of System Administrators.
TESISQUARE maintains an updated list of System Administrators ("SYSTEM ADMINISTRATOR") and complies with the requirements indicated in the Garante Privacy Provision of November 27, 2008. In particular, TESISQUARE proceeds with the designation of professional figures aimed at the management and maintenance of a processing system or its components, as well as administrators of databases, networks, security apparatuses, complex software systems and who in their usual activities are, in many cases, concretely "responsible" for specific work phases that may involve high criticality with respect to data protection. TESISQUARE also proceeds, at least annually, to audit the work of the SYSTEM ADMINISTRATOR.

Signing, by each employee, of a confidentiality agreement upon employment
At the time of employment TESISQUARE signs an agreement with its employees concerning the obligations of confidentiality and secrecy with regard to the confidential information of which the same employee has become aware as a result of or as a consequence of the employment relationship, this being deemed to be all information, data and documents of a confidential nature, that is, subject to industrial secrecy, owned by TESISQUARE or its subsidiaries or affiliates, as well as any other information of any nature learned from TESISQUARE's customers.

Record keeping of the owner or manager
Pursuant to Article 30 GDPR, TESISQUARE keeps a register of the owner and responsible person constantly updated on the basis of processing activities actually carried out. The preparation of the processing register is functional for compliance with the principle of accountability; compliance with security requirements; and the planning of how to respond to the exercise of data subjects' rights.
The registers contain all the information indicated in the aforementioned Art. 30 GDPR and are managed (as well as the other data protection fulfillments) by a special management platform.

Privacy policies and procedures

TESISQUARE has a robust set of procedures and policies related to the processing of personal data that it performs both as Data Controller and as Data Processor. These policies are discussed and approved by the internal Privacy team, the Privacy Committee, the Data Protection Officer, and other corporate figures and entities that may be impacted.

Regular meetings of an internal privacy committee
TESISQUARE has an internal Privacy Committee in which the company figures most involved on the issue and the DPO take part, for alignment and discussion on cross-cutting issues.

Appointment of a DPO
TESISQUARE has appointed a data protection officer (DPO) who can be contacted at the email address: dpo@tesisquare.com.

Privacy by design and impact assessments
TESISQUARE, in compliance with Article 25 GDPR, has prepared its own methodology for the analysis and assessment of processing, so that from the design of the processing, appropriate technical and organizational measures are determined and implemented to effectively implement the data protection principles and necessary safeguards to meet the requirements of the Regulation and protect the rights of data subjects.
Pursuant to Articles 35 and 36 of the GDPR and based on the document WP248 - Guidelines on Data Protection Impact Assessment adopted by WP art. 29, TESISQUARE has also prepared its own methodology for the analysis and assessment of processing operations that, given the nature, object, context and purpose of the processing, present a high risk to the rights and freedoms of natural persons in order to carry out the assessment of their impact on the protection of personal data before the processing begins.

Periodic third-party audits
TESISQUARE periodically organizes surveillance actions by external audit figures, in order to detect observations/points of attention/non-compliance that enable the organization to work on time to refine and strengthen certain aspects that are vital to the full transposition of the GDPR and regulations governing data protection aspects.

Privacy policies
The company prepares, in compliance with Art. 13 and 14 GDPR, notices to data subjects to provide information on the purposes and methods of processing, where their data are collected. Such processing is based on the principles of fairness, lawfulness, transparency and protection of the confidentiality and rights of data subjects.

The main policies are:

1. Privacy policy for applicants
2. Privacy policy for customers
3. Privacy policy for suppliers
4. Privacy policy for Tesisquare website
5. Whistleblowing privacy policy
6. Marketing policy

Other disclosures are prepared from time to time if the company undertakes any new processing of personal data as Data Controller.

ISO 27001 certification
TESISQUARE is UNI CEI EN ISO/IEC 27001:2017 certified and maintains an Information Security Management System (ISMS) certified by periodic third-party audits.

4 Technical measures to ensure GDPR compliance

TESISQUARE maintains a program technical measures designed to protect its own and Clients' data from accidental or unlawful loss, access, or disclosure, as well as designed to identify reasonably foreseeable internal security risks and unauthorized network access and minimize security risks.

Logical access authorization
TESISQUARE defines access profiles with respect to the minimum privilege necessary to perform the assigned tasks. Authorization profiles are identified and configured prior to the start of processing, so as to limit access to only the data necessary for the performance of processing operations.
These profiles are subject to periodic audits aimed at verifying the existence of the conditions for the preservation of the assigned profiles.

Incident Management
TESISQUARE has implemented a specific Incident Management procedure in order to ensure that normal service operations are restored as quickly as possible, ensuring that the best service levels are maintained.

Data Breach
TESISQUARE has implemented a specific procedure aimed at the management of events and incidents with potential impact on personal data that defines roles and responsibilities, the process of detection (alleged or established), the application of law enforcement actions, the response and containment of the incident/violation as well as the means by which to notify the Client of personal data breaches.

Malware protection
Systems are protected from intrusion and program action by the activation of appropriate electronic tools that are updated regularly.

Authentication credentials
The systems are suitably configured to allow access only to individuals with authentication credentials that uniquely identify them. These include, code associated with a password, confidential and known only by the same; authentication device owned and used only by the user, where access is permitted only with an identification code and password.

Password
With regard to the basic characteristics i.e., requirement to change at first access, minimum length, absence of easily traceable elements of the subject, rules of complexity, expiration, history, contextual evaluation of robustness, display and storage, the password is managed

according to best practices. Those to whom credentials are assigned are given instructions on how to ensure secrecy.

Logging
Systems are configured to allow tracking of access and, where appropriate, of activities performed by different types of users (administrator, super user, etc.) protected by appropriate security measures to ensure their integrity.

Backup & restore
Appropriate measures are taken to ensure that access to the data is restored in the event of damage to the data or electronic tools, within a time frame compatible with the rights of the data subjects.

Vulnerability Assessment & Penetration Test
TESISQUARE, through third parties, periodically carries out vulnerability analysis activities aimed at detecting the state of exposure to known vulnerabilities, both in relation to infrastructural and application domains.
Where deemed appropriate in relation to the potential risks identified, these checks are periodically supplemented with specific Penetration Testing actions, through intrusion simulations using different attack scenarios, with the objective of verifying the security level of applications/systems/networks through activities aimed at exploiting the detected vulnerabilities to bypass physical/logical security mechanisms and gain access to them.
The outcomes of the audits are promptly and in detail reviewed to identify and implement improvement points necessary to ensure the required high level of security.

Firewall
Personal data is protected from intrusion through next-generation firewalls kept up-to-date with the best available technologies.

Security on communication lines
The hosting service providers selected by TESISQUARE have secure communication protocols in line with what technology makes available

Network security
TESISQUARE will maintain access controls and policies to manage what access is allowed to the network from each network connection and user, including the use of firewalls or functionally equivalent technologies and authentication controls.
TESISQUARE will maintain corrective action and incident response plans to respond to potential security threats.

5 Physical measures to ensure GDPR compliance

Physical access controls
The physical components of TESISQUARE software solutions are housed in anonymous structures (the "Facilities"). Physical barrier controls are used to prevent unauthorized entry to the Facilities at both the perimeter and building access points.

Passage through physical barriers at the Facilities requires electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contracted or in-house security guard service, receptionists, etc.).
Employees and contractors are issued photo identification badges that must be worn while employees and contractors are in any of the facilities.
Visitors are required to check in with designated personnel, must display proper identification, are assigned a visitor identification badge that must be worn while the visitor is in any of the facilities, and are continuously escorted by authorized employees or contractors while visiting the facilities.

Limited access by employees and contractors
TESISQUARE provides access to Facilities to those employees and contractors who have a legitimate business need for such access privileges.
When an employee or contractor no longer has a business need for the access privileges assigned to them, the access privileges are promptly revoked.

Physical security protections
All access points (other than main entrance doors) are maintained in a protected (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all persons accessing the Facilities.
TESISQUARE also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring of vulnerability points (e.g., primary entrance doors, emergency exit doors, roof hatches, dock doors,
etc.) with door contacts, glass-breaking devices , internal motion detection or other
devices designed to detect people attempting to gain access to Facilities

6 Transfer of data to countries outside the EEA

TESISQUARE stores and processes its customers' data as a Data Processor under Article 28 of GDPR only in European data centers or otherwise located within the European Economic Area.
Some processing activities necessary to deliver services to the Customer (for example, activities that fall within consultancy or IT projects) may be processed by personnel of TESISQUARE Group companies located in countries outside the EEA (to date, Albania and the United States). Such processing within the Group is tracked, governed by special agreements with reinforced clauses (so-called "standard contractual clauses" drafted by the EU Commission) and subject to technical security measures.