DOCUMENT TITLE:	Data Protection Policy
DRAFTED AND APPROVED BY:	Legal Affairs Department
VERIFIED BY:	Human Resources and Organization Department Digital Transformation & Information Technology Department Internal Auditing
ISSUE DATE:	February 2026
UPDATE DATE:	June 2026
NO. OF PAGES:	9
NO. OF ANNEXES:	0

TABLE OF CONTENTS

1. Introduction and Reference Legislation

Taking into consideration the legal framework regarding personal data protection (consisting mainly of Regulation (EU) 2016/679 "GDPR" or "Regulation" and Legislative Decree No. 196/03 and subsequent modifications and additions "Privacy Code"), the OVS Group recognizes that the correct management of personal data represents a value of fundamental importance, to which specific paragraphs of the Code of Ethics of OVS S.p.A. are dedicated (in particular, paragraphs 3.1.5 and 3.2.4 of the updated document available in the appropriate section of the website ovscorporate.it), and makes the utmost effort to ensure the protection of personal data collected and processed within its business activities.
This document outlines the key points on which OVS ("OVS" or the "Company") has based its data protection system as well as that in force at its subsidiaries, recalling the roles and responsibilities assigned by the Company within its business organization in compliance with the Regulation, Guidelines, recommendations and best practices of the European Data Protection Board (also known by the acronym "EDPB"), as well as the measures of the supervisory authority.

2. Management System

2.1 Roles and Responsibilities

2.1.1 Data Controller

The Data Controller of personal data (hereinafter "Controller") is identified as the legal entity in whose interest the processing is performed and which determines the purposes and means of such processing (i.e. OVS and/or another OVS Group company). Processing under the Regulation means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
The Controller is responsible for decisions regarding the purposes, methods of personal data processing, and the tools used, including the security profile, and is responsible for ensuring compliance with data protection legislation.

2.1.2 Data Protection Officer

The Data Protection Officer (hereinafter "DPO") is the person designated by the Controller through a resolution of the Board of Directors who, pursuant to Article 39 of the Regulation, performs an information and advisory function on the main obligations provided for by the Regulation.
In particular, the DPO is tasked with informing, advising, and collaborating with all corporate

organizational structures in the management of data protection issues, monitoring compliance with applicable regulatory requirements and the Controller's policies, as well as acting as a point of contact for the Supervisory Authority (also known as the "Privacy Guarantor") and for data subjects.
Provided they are compatible with the role, the Controller may assign further tasks and functions to the DPO including, but not limited to: (i) promoting a culture of data protection within the company and employee training; (ii) supporting the assessment of any new corporate project according to the principles of Privacy by design and Privacy by default; (iii) supporting the assessment in the event of a personal data breach presenting a high risk to rights and freedoms and in subsequent activities (e.g. notification to the Supervisory Authority and possible communication to data subjects).
The contact details of the DPO – including the dedicated channel responsabileprotezionedati@ovs.it – are published on OVS websites, in privacy notices, and are also brought to the attention of the corporate organization through publication on the company intranet. In addition, the contact details of the DPO are communicated to the Supervisory Authority.
OVS has also defined the information flows to and from the DPO. In particular, in order to ensure full autonomy and independence in the performance of their functions, the DPO reports at least once a year to the Control, Risk and Sustainability Committee and to the Board of Directors on the level of compliance with the Regulation, reports on compliance with applicable legislation and corporate data protection policies, and on the outcome of the monitoring activities carried out, formulating, if necessary, suggestions for improving internal compliance. In addition, the DPO may be convened at any time by the Board of Directors and, in turn, may request to be heard should they see the need to report on issues relating to data processing and/or compliance with the Regulation and/or applicable legislation on the processing of personal data.

2.1.3 Persons Authorized to Process Data

The Authorized Persons are the natural persons within the corporate structure assigned, in the exercise of their duties, to specific tasks and functions connected to personal data processing operations contained in databases and in corporate paper archives.
The Authorized Persons carry out their activities in accordance with the instructions received and corporate policies and, in any case, operate under the responsibility of the Controller (pursuant to Article 2 quaterdecies of the Privacy Code).
Within the framework of the Regulation's provisions, OVS has set up a training program regarding personal data processing. The training is carried out through self-learning via mandatory training modules, available on the corporate portal dedicated to training. More specifically, the training path requires the completion of two modules, "basic" and "advanced", the learning of which will be subject to verification by means of a test, upon passing which a certificate of completion of training will be issued.
In order to ensure a greater and more effective peripheral oversight in privacy management, OVS has also established an internal committee composed of, in addition to the corporate DPO, representatives (so-called "Privacy Champions") of the Legal Affairs Department and of each other corporate function most involved in personal data management processes, with support,

coordination, and guidance tasks and duties.

2.1.4 System Administrators

The System Administrator ("SA") is the individual who, equipped with appropriate technical skills, is in charge of managing and maintaining a data processing system or its components. Given the technical peculiarities, the SA holds an extremely sensitive role: they design, develop, and manage the network infrastructure, servers, software, and basic application services, often dealing with the security and protection of data and resources. Furthermore, they provide technical and IT support on software and hardware.
The SA is designated by an appointment conferred by the Controller containing an analytical list of requirements and skills as well as the areas of operation permitted based on the assigned authorization profile.
The appointment signed by the SA is placed within the employee's personal file and in the archives of the Digital Transformation & Information Technology Department ("IT Department") of the Company for the processing and/or updating of the list of assigned individuals.

2.1.5 Data Processors

Whenever a service contract is concluded that involves the processing of personal data for which OVS is the controller, the IT Department conducts a supplier qualification procedure in order to verify, through the completion of a specific checklist, that the latter possess sufficient guarantees, have adopted appropriate technical and organizational measures, and that the processing meets the requirements of the Regulation and ensures the protection of the data subject's rights.
Once the verification procedure has been passed, the suppliers are designated as data processors (pursuant to Article 28 of the GDPR) and are required to sign a specific "Appointment as Data Processor" which will form an integral part of the contract and contains the instructions on processing, the violation of which results in the application of contractual remedies in compliance with the provisions of the Regulation, national legislation, and applicable measures of the Supervisory Authority.
The "Appointment as Data Processor" template is prepared and kept updated by the Legal Affairs Department which, with the intervention of the DPO, also deals with any support that may be necessary during the compilation and/or negotiation of the appointment with suppliers.
Each corporate Department undertakes to maintain a register of contracts (so-called "Privacy Repository") in which contracts and related Appointments as Data Processor are archived.
Each departmental Privacy Repository is accessible to the Privacy Champion of the department and to any other delegates designated by the Function Manager, as well as to the privacy representative of the Legal Affairs Department and the DPO.

2.2 Record of Processing Activities

The obligation to prepare and keep updated the Record of processing activities (the "Record") is provided for by Article 30 of Regulation (EU) 2016/679 ("GDPR"), which distinguishes between the Record to be kept by the Data Controller (Article 30.1 GDPR) and that of the data processor (Article 30.2 GDPR). The Record represents an accountability tool, essential for maintaining an

updated overview of the processing currently carried out by the corporate organization.
The process of periodic updating of the OVS Record is carried out by a multidisciplinary team composed of the DPO, the privacy representative of the Legal Affairs Department, and the representatives of the IT Department, the latter as the entity responsible for maintaining the Records according to internal OVS procedures. In particular, at least annually, the Privacy Champions collect the information and subsequently complete the census form for the processing carried out by the respective corporate department. The census forms are subject to verification by the DPO and the privacy representative of the Legal Department and, once validated, are transmitted to the IT Department to update the Record.
In addition to the periodic update process, if new processing operations are introduced and/or a processing operation already carried out by the Controller is significantly modified, entailing the obligation and/or necessity of an impact assessment, the Record is updated as soon as the related impact assessment is validated.

2.3 Management of Risk Arising from Personal Data Processing

2.3.1 Data Protection Impact Assessment

In order to ensure compliance with the principles of data protection by design and by default pursuant to Article 25 of the GDPR, OVS has adopted a strategic and preventive approach based on assessing the risk of potential infringement of the rights and freedoms of the data subject both in the context of new processing operations and in the event of a significant variation of a processing operation already carried out. If a certain processing operation presents a high risk to the rights and freedoms of natural persons, the Controller, with the support of the DPO, proceeds to draft a Data Protection Impact Assessment ("DPIA" pursuant to Article 35 of the GDPR).
The process of drafting, validating, and controlling the DPIA is established in a specific internal procedure and involves the representatives of the corporate functions responsible for the processing under evaluation. In particular, the process is divided into phases and is introduced by the compilation of a checklist to assess the obligation and/or necessity of carrying out a DPIA in compliance with regulatory requirements and the guidelines of the Privacy Guarantor. If the need to carry out a DPIA is identified, the Controller is required to consider the criteria of necessity and proportionality, identify and assess the risks in terms of personal data protection, as well as possible solutions to mitigate these risks. Once validated and signed, the DPIA is subject to periodic review.

2.3.2 Management of IT Security Incidents and Data Breaches

OVS has identified within a specific policy available on the corporate intranet the activities to be carried out to manage security incidents, whether of an IT nature and/or relating to personal data protection regulations.
"IT Security Incident" means the single event or series of unwanted or unexpected events that indicates a possible breach of information security, policies, or a failure of controls, and which have a significant probability of compromising business operations and threatening information security; "Privacy Incident" or "Personal Data Breach" ("Data Breach") means an IT Security Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized

disclosure of, or access to, personal data transmitted, stored, or otherwise processed by the Controller.
The procedure adopted by OVS foresees the following security incident management process:

- **Detection of anomalous events, determination of the nature, and reporting of the event:** all users who directly or indirectly detect an anomaly must immediately report it to the IT Department.
- **Determination of the type of incident:** The IT Security Manager, with the support of the IT Security team and the possible collaboration of the Legal Affairs Department, based on the elements collected, classifies the incident according to the severity level.
- **Risk analysis for the rights and freedoms of data subjects:** The DPO, in collaboration with the IT Security team, assesses the presence of risks to the rights and freedoms of data subjects arising from personal data processing capable of causing physical, material, or non-material damage;
- **Assessment of any need for communication to external parties:** depending on the level of risk to the rights and freedoms of data subjects, it is necessary to assess which of the following External Reports must be prepared;
- **Resolution of the IT Security Incident:** the IT Department, in collaboration with the Departments involved, implements the appropriate countermeasures based on the event that occurred;
- **Verification of the restoration of normal operations and closure of the incident:** in order to ensure an effective return to normal corporate operating conditions, the IT Security team verifies the adequacy of the actions taken and the complete restoration of the security of the impacted environments;
- **Preparation of Internal Reporting:** the IT Security team is responsible for formalizing all information collected during the different phases of incident management, preparing the Internal Reporting that addresses all aspects.

2.4 Transfer of Personal Data

2.4.1 Intra-group Transfer of Personal Data

If the transfer of personal data is linked to the provision of intra-group services, the relationship between OVS Group companies must be contractually regulated through the signing of a specific "Appointment as Data Processor" pursuant to Article 28 of the GDPR.
In the absence of an exchange of services, the transfer of personal data between OVS Group Companies established in the European Economic Area, including those of customers and employees, may be permitted for internal administrative purposes, and linked to processing related to the ordinary support activities for Group companies that do not pose high risks to data subjects.

2.4.2 Transfer of Personal Data to Third Countries or International Organizations

The transfer of personal data to third countries or international organizations can only take place if the Controller and/or the data processor comply with the conditions and requirements set out in the Regulation.
In the event that the Controller plans to transfer personal data to countries outside the European

Union or to international organizations, the DPO is consulted in advance to ensure that the transfer takes place in compliance with the provisions of the Regulation.

2.5 Requests to Exercise Rights by Data Subjects

Regulation (EU) 2016/679 provides that data subjects, i.e. the persons whose data are processed by the Controller (the "Data Subjects"), may exercise specific rights pursuant to Articles 15 to 22 of the GDPR.
OVS has defined in a specific internal procedure available on the corporate intranet the methods for managing requests to exercise rights by Data Subjects in order to ensure their correct identification and timely fulfillment according to the terms of the Regulation by the functions involved.

2.6 Audit

The Regulation assigns to the Controller the task of implementing appropriate technical and organizational measures to ensure that personal data processing is carried out in compliance with current regulations, and the Controller must also be able to demonstrate this in a documented manner according to the accountability principle.
In compliance with the provisions of letter d) of Article 32 of the GDPR, the overall organization and Privacy management system of the OVS Group, or parts thereof, as well as the technical and organizational measures are periodically and cyclically subjected to control and verification by the Internal Audit Function or by appointed third parties, in order to ensure correct implementation and application, adequacy due to the complexity of the organization and the processing carried out, as well as adherence to the regulatory framework.

2.7 Consequences of Non-Compliance with Data Protection Regulations

The organizational system of the OVS Group defines rules and processes and ensures their implementation and traceability in accordance with the accountability principle.
Failure to comply with processing instructions or, more generally, with corporate regulations on personal data protection may lead to the opening of disciplinary proceedings by the Human Resources and Organization Department, which could end with the issuance of measures commensurate with the seriousness of the violation.