Omnidea's Privacy and Security Policy

Technological and Organizational measures

1. CONFIDENTIALITY: Measures to prevent any illegitimate access
   - 1.1. Encryption. For all corporate devices the XTS-AES-128 encryption of mass memories is enabled. Access to web services through non-encrypted protocol is inhibited. WiFi connection is protected via WPA2 protocol. At the application level, encrypted protocols such as HTTPS, SFTP and SSH are used. Remote accesses take place exclusively via VPN.
   - 1.2. Physical access to systems, facilities, paper archives, data center. The paper archive was eliminated in favor of replacement preservation PDF / A on Data Center Cloud compliant with ISO / IEC 27001, ISO / IEC 27017, ISO / IEC 27018, AICPA SOC 2/3, PCI DSS. The corporate premises are protected by a video surveillance system.
   - 1.3. Logical access to systems and data. Access to IT systems, databases, applications, data and file servers is protected and managed with specific utilities and permits, according to the principle of the minimum privilege.
   - 1.4. Password policy. Multi-factor authentication enabled for all company accounts; SSO with Google Company Account; verification of the password complexity for all services; Periodic control automated for the robustness of the passwords used.
   - 1.5. Separation control. Separation in distinct databases; Separated environments for testing, development and production are used; Access to data is managed through specific users.
   - 1.6. Definition of tasks and roles. Matrices of access to systems and data are defined. Accesses are checked and recorded via Access Log and a hierarchy for IT administrators, DB administrators, developers and operators is managed.
   - 1.7. Data and equipment disposal. Paper material eliminated by means of obstructions; Mass memories of corporate devices are formatted by multiple overwrite before dismissed; Remote Wipe for lost or stolen devices.

2. INTEGRITY: Measures to prevent undesired modifications
   - 2.1. Transmission control. At the application level, encrypted protocols such as HTTPS, SFTP and SSH are used. Remote accesses take place exclusively via VPN. Centralized antivirus and quarantine system for mail management.
   - 2.2. Input control. The platforms used include reversal, tracking and control of the integration and manipulation of the TATI.
   - 2.3. Monitoring and traceability. The platforms used include logging procedures for tracking and monitoring events. Logs are available to ensure integrity and detect events that may have compromised data or systems.

3. AVAILABILITY: Measures to prevent data loss
   - 3.1. Backup and restore policy. Automatic Backup on Data Center Cloud Compliant with ISO / IEC 27001, ISO / IEC 27017, ISO / IEC 27018, AICPA SOC 2/3, PCI DSS. Global e-discovery system (Google Vault) by email, file and chat. Retention period: 10 years.

Omnidea S.r.l.
Via Niccolò Tommaseo, 94
35131 Padova

3.2. Business Continuity Plan. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
3.3. Disaster Recovery Plan. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
3.4. Capacity Planning. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.

4. SECURITY: Measures to prevent explicit violations of personal data
4.1. Privacy and/or Security Regulations. Privacy policy available on our website; Security Policy for shared internal use with new assumptions. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
4.2. Roles for the management and the security of information systems. Organization chart related to key features available.
4.3. Training in the area of privacy and/or security. Updates regarding privacy and security for employees are organized periodically. Last course carried out in May 2021.
4.4. Supply Chain Security Management. We verify providing and consultants regarding legal aspects and GDPR.
4.5. "Smart Working" Security Policy. At the moment the staff does not carry out activities in "Smart Working". Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
4.6. Information System Asset Inventory. Managed via MDM platform for corporate devices.
4.7. Risk analysis for information systems. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
4.8. Incident Management. Expected an incident management system assisted by e-discovery platform (Google Vault). Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
4.9. Data Breach Procedure. Present a tracking and management system of the Breach data as required by the GDPR. Any date breaches are communicated within 72 hours of interested parties, including nature of the violation, probable consequence and measures adopted to mitigate its effects.
4.10. Data Loss Prevention. DLP rules for corporate content shares (Google Workspace Enterprise). For all corporate devices the XTS-AES-128 encryption of mass memories is enabled. Mobile devices can be remotely deleted via MDM management platform.
4.11. Vulnerability Assessment, Penetration Test. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.
4.12. Firewall, IDS, IPS. Present Firewall managed by the connectivity provider for the corporate network; Employee devices include a personal firewall: our activities are based on SaaS platforms that respond to the highest levels of reference and in particular the ISO 27001 standard.

Omnidea S.r.l.
Via Niccolò Tommaseo, 94
35131 Padova

4.13. Malware and Spam protection. Google Workspace Enterprise antispam systems, corporate domain configured with SPF, DKIM and DMARC policy.
4.14. Data Leak Prevention. DLP rules for company content shares (Google Workspace Enterprise); Periodical reports to directors related to the sharing of external data to the organization.
4.15. Patching and updates management. Centralized via MDM for business devices for the operating system; Application software exclusively in SaaS mode.
4.16. System Administrator Log. The registration of access systems are maintained, as required by the provision of the guarantor for the protection of personal data of 11/27/2008.
4.17. Test and audit. Our activities are based on SaaS platforms that respond to the highest reference standards and in particular the ISO 27001 standard.

Last modified: February 25, 2022

Omnidea S.r.l.
Via Niccolò Tommaseo, 94
35131 Padova