Technical and Organizational Measures

This document is an integral part of the Agreement (as defined in Clause 1.1. (e) of the General Licensing Conditions).
The Customer represents and warrants that the technical and organizational measures set out in the Terms of Processing and Technical and Organizational Measures are appropriate for PRIMAVERA to process the data on its behalf.

Security of Processing

PRIMAVERA shall implement the appropriate technical and organizational measures to ensure a level of security for the personal data processed for its own purposes and in the name and on behalf of the Customer. These technical and organizational measures to be adopted in processing activities carried out by PRIMAVERA in the name and on behalf of the Customer are defined in accordance with the information entered by the Customer in the Terms of Processing and the regular use of the software and its features pursuant to the Agreement.
Considering the Software and Service provided to its customers, PRIMAVERA has defined a set of SPECIFIC MEASURES that shall be adopted for each level of service:

SECURITY	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
Strong password policy Strong password policy for Users and application administrators	●	●	●	●	●	●	●
Multi-factor authentication Authentication of all users can be done by two or more factors, for example password and confirmation on smartphone	●	●	●	○	○	○	○
Self-expiring credentials User credentials expire over time	○	○	○	●	●	○	○
Inactivity notice and date of last access Identifies users inactive for more than x days and reports last access date	●	●	●	○	○	○	○
Date, time, and IP address of the last access Logs containing information on users' last access to applications/services	●	●	●	●	●	●	●

SECURITY	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
Regular External Audits Audits, penetration, and vulnerability testing performed by entities outside the infrastructure where the applications are installed.	●	●	●	●	●	●	●
SOC – Security Operations Center 24x7 The relevant systems are monitored by security teams working 24/7.	▨[1]	▨[1]	▨[1]	●	●	▨[1]	●
Antivirus The systems have installed and updated antiviruses	●	●	●	●	●	●	●
Use of TLS latest version The communications between the different systems use the most modern information encryption protocols	●	●	●	●	●	●	●
Encrypted passwords All credentials stored in code, configuration files or in databases are at least HASP-256 encrypted	●	●	●	●	●	○	●
Encrypted data at rest The systems use at least one type of information encryption: FileSystem, Database or Full Disk	●	●	●	●	●	●	●
Encrypted/anonymized personal information in the BD Personal data on BD or files are encrypted or anonymized	●	●	●	○	○	○	○
URL with no visible variables All URLs are free of session variables and personal data	●	●	●	●	●	●	●
No personal information is stored beyond the session No personal information is stored on the browser, disk, or memory, as cookies for instance, beyond the duration of the session and only strictly as necessary	●	●	●	●	●	●	●
Secure password transmission Credentials transmitted in HASH minimum SHA-256	●	●	●	●	●	●	●
Encrypted communications Secure session with SSL/TLS or HTTPS security protocol	●	●	●	●	●	●	●
Secure communication between layers Communication with FE or DB layers via secure session	●	●	●	●	●	●	●
Use of good DNSSec, SPF, DKIM, fixed IP practices ... Ability to ensure the correct identity of the sender and recipient of the data transmission.	●	●	●	●	●	●	●
DoS protection Protection against denial-of-service (DoS) type attacks	●	●	●	●	●	●	●

SECURITY	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
Perimeter protection Use of firewalls and other threat detection tools in perimeter defense	●	●	●	●	●	●	●
Detection of malicious activity Use of IDS to monitor and detect malicious activity or security policy breaches	●	●	●	●	●	●	●
CRUD logs Logs are kept with information about the actions performed on the data (create, read, update, delete)	▨[2]	▨[2]	▨[2]	▨[2]	▨[2]	▨[2]	▨[2]
Social engineering tests Regular security training and social engineering activities carried out with all PRIMAVERA employees	●	●	●	●	●	●	●
Log integrity Logs are stored in READ mode only with integrity assurance	●	●	●	●	●	●	●
Access logs Logs of access activities and failed attempts	●	●	●	●	●	●	●
Session timeout End-of-session policies for remote endpoints and applications	●	●	●	●	●	●	●

BACKUP & RECOVERY	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
Backup policy Backups are made for all stored Data	●	●	●	●	●	●	●
Secure Data Storage on the Device Encryption and digital signature for backups	●	●	●	●	●	●	●
Offsite backup Backups made for different physical locations at least weekly	●	●	●	●	*[1]	●	●
Backup tests Backups and backup replacement procedures are regularly tested via tests in place	●	●	●	●	●	●	●

FRAMEWORKS	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
ITIL	●	●	●	●	●	●	●
SCRUM	●	●	●	●	●	●	●
ISO9001	●	●	●	●	●	●	●
CMMI	●	●	●	●	●	●	●

DATACENTER	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
ISO 20000	●	●	●	●	●	●	●
ISO 22301	●	●	●	●	●	●	●
ISO 27001	●	●	●	●	●	●	●
ISO 27017	●	●	●	●	●	●	●
ISO 27701	●	●	●	●	●	●	●
ISO 27018	●	●	●	●	●	●	●
ISO 9001	●	●	●	●	●	●	●
SOC 1, SOC 2 & SOC 3	●	●	●	●	●	●	●

DATACENTER	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
GDPR	●	●	●	●	●	●	●
EU-US Privacy Shield	●	●	●	●	●	●	●
EU Model Clauses	●	●	●	●	●	●	●
EN 301 549 (EU)	●	●	●	●	●	●	●
ENISA IAF (EU)	●	●	●	●	●	●	●

SLAs	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	SaaS Dedicado	Omnia v2	Omnia v3
Availability >= 99,5% month	●	●	●	●	*[2]	●	●
Support tickets response time	**From 12h for “Critical” tickets; up to 24h for “Planning” tickets** (Mainland Portugal times)	**From 12h for “Critical” tickets; up to 24h for “Planning” tickets** (Mainland Portugal times)	**From 6h for “Critical” tickets; up to 18h for “Planning” tickets** (Mainland Portugal times)	**From 12h for “Critical” tickets; up to 24h for “Planning” tickets** (Mainland Portugal times)	**From 6h for “Critical” tickets; up to 18h for “Planning” tickets** (Mainland Portugal times)	**From 6h for “Critical” tickets; up to 18h for “Planning” tickets** (Mainland Portugal times)	**From 6h for “Critical” tickets; up to 18h for “Planning” tickets** (Mainland Portugal times)

● Yes

○ No

▨[1] The service is supported on PaaS so monitoring is carried out directly by Microsoft

*[1] Remote backup can be ensured by the Partner as frequently as the latter may determine

▨[2] Not all operations or tables have logs and in certain instances activating those logs falls to the customer/Partner

*[2] Since the service is partially controlled by the PRIMAVERA Partner it is not possible to guarantee the SLA, although it is guaranteed in terms of infrastructure availability.