TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The description of the technical and organizational measures Centric Software has implemented are listed below.

Customer is entitled to subscribe to changes to obtain notice of updates implemented by Centric to those measures.

The technical and organizational measures may also be completed by specific terms as detailed in the documentation associated to each release of the software products and/or services ordered by Customer.

1. **Confidentiality** (**Article 32**(**1**) **lit.** (**b**) **GDPR**)

- Physical Access Control

No unauthorised access to Data Processing Facilities

- Issue of physical keys to authorized personnel with a need to access applicable facility(ies);
- Door locking of facilities to prevent unauthorized access;
- All visitors are collected at reception, accompanied while on-site, and limited to areas necessary for the purpose of their visit
- Office doors and windows closed when workers are not in the facility.
- Electronic Access Control to systems

No unauthorised use of the Data Processing and Data Storage Systems

- Authorization concept where access to systems is provided on a need to know basis;
- Defined process for allocation of user accounts;
- Computers and mobile devices secured by password;
- Securing of network connections (e.g. remote access).
- Internal Access Control (permissions for user rights of access to and amendment of Personal Data)

No unauthorised Reading, Copying, Changes or Deletions of Personal Data within the system

- Differentiated access rights (profiles, roles, transactions and objects)
- Rights authorisation concept based on need to know.
- Isolation Control

The isolated Processing of Data, which is collected for differing purposes

- Data segregated by function (maintenance support / consulting services / hosting services)

- Keeping customer data separate (though may be stored on the same systems) to enable customer to exercise rights regarding deletion.

2. **Integrity** (**Article 32**(**1**) **lit.** (**b**) **GDPR**)

- Data Transfer Control

No unauthorised Reading, Copying, Changes or Deletions of Personal Data with electronic transfer or transport

- Encryption/tunneling (Virtual Private Networks (VPN))
- Utilization of secure FTP
- Data Entry Control
- Differentiated access rights (profiles, roles, transactions and objects) by Agent personnel

3. **Availability and Resilience** (**Article 32**(**1**) **lit.** (**b**) **GDPR**)

- Availability Control

Prevention of accidental or willful destruction or loss

- Email backups
- Backups of data logged into the support services portal
- Where Hosting Services are being provided, options for backup strategy and disaster recovery are available to customer for data they input into the Licensed Software
- Worker computers have anti-virus software
- Firewall systems
- Rapid Recovery (Article 32(1) lit.(c) GDPR) (disaster recovery plan)
  - Disaster recovery plan for all key Agent business systems
  - Disaster recovery options available for Principal where Hosting Services have been ordered and paid for.

4. **Procedures for regular testing, assessment and evaluation** (**Article 32**(**1**) **lit.** (**d**) **GDPR; Article 25**(**1**) **GDPR**)

- Annual penetration and security vulnerability testing of Centric8 PLM software
- System monitoring of critical Centric Software systems

- System monitoring of Customer systems being hosted through Centric Software's Hosting Services
- Incident Response Management
- Order or Service Agreement Control

No third party data processing as per Article 28 GDPR without corresponding instructions from the Client

- Controls on the selection of the Service Provider, duty of pre-evaluation;
- Availability of resources to discuss with Customer third party data processing scope;
- Customer may request access to evaluate third party data processing protections.

5. **Data Protection by Design and Default** (**Article 25** (**1**) **and** (**2**) **GDPR**)

Agent reasonably limits use of personal data and internal access to Customer personal data to that necessary for each specific purpose of processing.

The Centric8 PLM software has enabled data encryption during transmission.

The Centric8 PLM software can also encrypt data stored within it at rest upon Customer's election. Customer must make this election in writing.