Audit Report Summary

Prepared for:

Fabasoft Austria GmbH
Honauerstraße 4,

4020 Linz, Austria

Fabasoft AG, Linz, has been audited by DHC GmbH on 3 August 2016. The objective of the audit was to verify that the Fabasoft Quality Management System is capable of providing Fabasoft's Services and Software Products with the quality required by companies in GxP-regulated industries (i.e. Pharmaceutical Industry and Supplier of Medical Devices).

During the audit, the Fabasoft managements systems for Quality Management (ISO 9001), IT Service Management (ISO 20000) and IT Security Management (ISO 27001) have been inspected.

Summary of Audit Results:

- **The quality management system, the IT service management system and IT Security management of Fabasoft is capable of providing products and services that are able to satisfy the requirements of customers in the GxP regulated industries.**
- **This applies equally to the processes applied during development of the software and to the processes of supplying the software in a private cloud as SaaS.**

The following processes have been inspected during the audit:

- Quality Management System
- Documentation Control
- IT Security Management
- Operational Change Management and Configuration Management
- System Maintenance and Support
- System Development Process.

The audit has been performed in the form of interviews based on a predefined questionnaire taking into account the processes mentioned above.

Documents provided by Fabasoft have been inspected to provide evidence that the required processes are established and managed so as to achieve the intended results in accordance with the quality policy and strategic direction of Fabasoft.

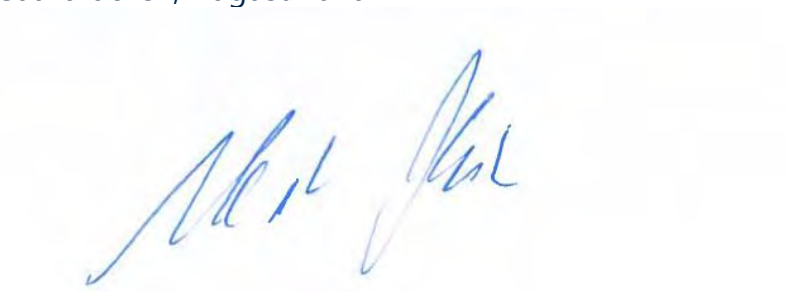
A full audit report has been generated based on the completed questionnaire; the list of documents inspected is provided as annex.

Remark

A GxP-regulated company using Fabasoft's products and services is still responsible for:

- Documenting the supplier evaluation process (probably referring to this report);
- Providing documented evidence that the used products and services fulfill the requirements for the specified intended use consistently;
- Having a written contract covering the outsourced activities in compliance with applicable GxP-regulations;
- Monitoring the performance of the service provider and the fulfillment of the contract.

Saarbrücken, August 2016



Dr. Stephan Müller
DHC Dr. Herterich & Consultants GmbH

Annex: General Compliance Requirements for Outsourced IT Services

Companies in the pharmaceutical industry and manufacturers of medical devices have to satisfy specific regulatory compliance requirements defined in law, EU GMP for pharmaceutical companies and 21 CFR for companies selling products in the United States. Depending on the countries where the products are marketed, additional regional legal requirements may apply.
Common to all these regional requirements is that the authorities controlling compliance with the requirements ask for documented evidence of compliance.
Particular requirements apply to IT systems used to support processes with relevance to product quality, patient safety, and data integrity. The same holds for outsourced IT services. For European pharmaceutical companies, such requirements are defined in EU GMP Annex 11 Computerized Systems. Requirements related to outsourced services, including IT services, are defined in EU GMP Chapter 7 Outsourced Activities.

Requirements for outsourced activities are:

- Before outsourcing, the regulated company must assess the capability of the service provider to make sure that it is capable of providing the requested services with the necessary quality.
- The regulated company is responsible for defining the responsibilities related to the outsourced service in a written contract (in general in form of a service level agreement or a quality agreement).
- The regulated company is responsible for monitoring and reviewing the outsourced services.

The overall responsibility toward authorities remains with the regulated company.

Requirements for Computerized Systems are:

- Validation of applications and qualification of the underlying IT infrastructure;
- Qualification of personnel appropriate to their designed duties;
- Definition and management of processes required for compliant operation of computerized systems, including:
    - IT Security Management,
    - IT Service Management.

These requirements with regard to outsourcing also apply to cloud-based services such as Software as a Service (SaaS).

Implementing and operating a cloud-based computerized system (SaaS) covers a three-step process

- **Step 1: Selection of Service Provider**

  In this step, the regulated company has to analyze its requirements for the computerized system and to evaluate the risk related to the system.

  Based on these results, potential supplier must be evaluated and assessed. The criterion for such an assessment is the capability of the potential suppliers to satisfy regulatory requirements. The assessment can be based on an evaluation of all available information on the potential suppliers, including certifications; it also can be based on a supplier risk audit.

- **Step 2: Establishment of Service and Computerized System**

  During this step, the computerized system is established. Activities also include validation of the system and qualification of the underlying infrastructure. In view of this, the regulated company can use documentation provided by the supplier in case this documentation is reviewed for suitability.

  Furthermore, the services needed to operate the system have to be defined. The responsibilities related to these services have to be defined; the duties and responsibilities of the service provider have to be defined in a written contract (Service Level Agreement).

- **Step 3: Operation of Computerized System**

  During operation of the computerized system, the regulated company has the responsibility for ensuring that the system stays in a validated state. This means that it has to provide documented evidence that the company is in control of the system.

  When operating a cloud-based system, there are processes which are under the responsibility of the regulated company, and processes which are under the responsibility of the service provider as defined in the service level agreement. The regulated company has to manage the processes on its own responsibility and to monitor the performance of the processes within the responsibility of the service provider.

DHC Dr. Herterich & Consultants | DHC Business Solutions GmbH & Co.KG
Landwehrplatz 6-7 | D - 66111 Saarbrücken

+49 681 93666 -0 | Fax -33
validation@dhc-gmbh.com
www.dhc-gmbh.com | www.dhc-vision.com

DHC AG
Bahnhofstrasse 1 6-7 | CH – 8180 Bülach

+41 43 411 40 -11 | Fax -10
info@dhc-ag.ch
www.dhc-ag.ch