Good Laboratory Practice

GUIDELINES FOR COLLABORATION WITH EXTERNAL IT SERVICE PROVIDERS SUPPORTING A GLP ENVIRONMENT

Release Date: 31.01.2018

Version: 2.0

TABLE OF CONTENTS

1 FOREWORD

The aim of the present document is to provide guidance on collaboration with external IT service providers supporting a GLP environment. The guidance should aid test facilities and promote the use of a common standard, but should not be considered as legally binding. The test facility management may use different approaches that are in compliance with the GLP Principles [1, 2]. The present guidelines may evolve according to experience over the next few years and may also depend on interpretations made by other OECD member countries.

The AGIT (**A**rbeits**G**ruppe **I**nformations**T**echnologie) is a working group consisting of representatives from Swiss GLP monitoring authorities and Swiss industry with the aim of proposing procedures, which are practical for use in test facilities fulfilling GLP regulatory requirements.

The Guidelines for Collaboration with External IT Service Providers Supporting a GLP Environment were issued as Version 1.0 in June 2016. This updated version (version 2.0) is in line with the OECD Advisory Document No. 17 (replacing OECD Consensus Document No. 10) [3].

2 INTRODUCTION

In the GLP environment, collaborations with external IT service providers are increasingly used in data capture, processing, storage and archiving, as well as IT infrastructure. Such collaborations, e.g. Software as a Service, should be in accordance with the OECD Principles of Good Laboratory Practice (GLP) and the relevant consensus and advisory documents concerning validation, operation, maintenance, retirement and archiving [2, 3, 4].

In many cases, a Service Level Agreement (SLA) is set up between the test facility and the external IT service provider. The SLA may be a separate document or part of a contract. The SLA's purpose is to define the responsibilities and expectations of both parties. Usually, SLAs cover technical aspects such as system availability, down time or fault repair. In order to fully support a GLP environment, additional considerations are necessary as outlined in this guideline.

3 SCOPE

This document gives guidance on specific requirements for the activities of and interactions with external IT service providers to support GLP compliance. External IT service providers are <u>not part of the test facility</u>. They may be a part of the same company as the test facility or a third party IT service provider. This collaboration should be defined in a SLA between the test facility and the external IT service provider.

Provided services might include, but are not limited to:

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS); e.g. network and hardware
- Platform as a Service (PaaS); e.g. storage, archiving and hosting
- Consultancy regarding validation of computerized systems

4 CONSIDERATIONS FOR AN SLA

4.1 Purpose of the SLA

The SLA is the central document defining all aspects of the collaboration between the GLP test facility and the external IT service provider. Besides the commercial aspects (e.g. financial, system availability), the SLA should address all relevant GLP aspects including but not limited to responsibilities, documentation, archiving, training, communication, reporting lines and audits. The quality system(s) used by the external IT service provider may or may not fulfil GLP expectations. Where the GLP expectations are not fulfilled in their entirety, the SLA should mandate that the IT service provider fulfills these needs.

4.2 Roles and Responsibilities

Since the scope of the test facility's SOPs does not include external IT service providers, the roles and responsibilities of both parties should be clearly described in the SLA.

Test facility management has the overall responsibility for GLP compliance for the life cycle of their computerized systems and for IT supporting services, even if external IT service providers provide these services. Test facility management may nominate a person within the test facility to take over defined responsibilities concerning the external IT service delivery.

The external IT service provider is responsible for the delivery of IT services in a way that the test facility is able to fulfil all applicable GLP requirements.

The external IT service provider should

- have personnel records of all employees directly involved in the services provided to the test facility as described in chapter 5
- document all activities performed on behalf of the test facility and ensure the traceability of these activities.
- provide access to documents on demand in case of inspections or audits as described in chapter 4.6 and 7
- archive documents as described in chapter 4.6

The SLA should ensure that the external IT service provider does not subcontract any part of the service to another external IT service provider without authorization by test facility management.

The SLA should allow audits/inspections by QA of the test facility and, if necessary, by GLP monitoring authorities.

4.3 System Life Cycle

If a computerized system is maintained and operated by an external IT service provider, the SLA should describe the duties of both the external IT service provider and the test facility during the life cycle of the supported system. This would include the system's validation, changes (hardware and software updates, migration, patches, incidents etc.), and retirement.

The SLA should explicitly address the handling of changes. Changes may be initiated by the test facility or by the external IT service provider. However, changes [5] affecting the validation status of a system should be authorized and released by the test facility management, and all associated documents should be archived in a GLP compliant archive [4]. Changes which have no impact on the validation status may be released by the external IT service provider, who is then responsible that these changes are appropriately documented and retained.

4.4 Security and Access Control

Appropriate technical and organizational measures should ensure the security and availability of both the data and systems. Maintenance of the systems and incident management should be addressed in the SLA.

The SLA should also cover the management of access rights. In any event, access to the system either at the test facility or at the IT service provider should be limited to trained personnel.

Example 1: The test facility personnel can perform user management for a software. The external IT service provider will rather do technical tasks for IT infrastructure, with appropriate access rights. In both cases, it is necessary to have an overview who has access to which parts of the system.

Example 2: If the IT service provider is providing archive services, then additional restrictions to the stored files may apply, (e.g. test facility management must authorize any transfers or deletions from the archive) [4].

4.5 Communication

Communication is a key factor for successful collaboration between the test facility and the external IT service provider. Both parties should agree in the SLA on the information to be shared (e.g. questions regarding incident and change management, contact person) and on the communication channels.

4.6 Documentation

The SLA should define which records are to be retained, the location of the records and their retention period. All documents and records of the external IT service provider should ensure the traceability to involved persons. All documents should be accessible by the test facility and/or GLP monitoring authority inspectors.

To ensure GLP compliance, minimum requirements for retention of documents and records are:

Type of records and documents	See also in chapter…	External IT service provider Retention period 10y	Test facility, GLP compliant archive Retention period 10y
SLA, contract	4	a	a
Personnel documents (CV, training records, job description)	5	a,c*	
Records of activities provided to the test facility	4.2	a	
Records regarding system life cycle of computerized systems	4.3	a,b*	b
Documentation of QA audits and reviews	6		a

a: 10 y after termination of SLA
b: 10 y after retirement of the computerized system
c: 10 y after the individual has left the company
* Whichever is earlier

5 PERSONNEL AND TRAINING

Personnel of the external IT service provider should be trained and have the appropriate experience to perform their job. The following documentation should be available, as a minimum, for each individual involved in the collaboration:

Personnel of the external IT service provider should be trained and have the appropriate experience to perform their job. The following documentation should be available, as a minimum, for each individual involved in the collaboration:

- **Curriculum Vitae (CV)** describing the basic education/training and professional experience
- **Training records** of continuing education, IT and Quality Management related, GLP awareness
- **Description of the current responsibilities** and roles (e.g. Job Description, organizational chart)

Personnel should be aware of GLP regulations and understand how these requirements are applicable to the services they perform in relation to the collaboration.

Specific GLP requirements in relation to IT services are, for example:

- GLP conform documentation [traceability, GLP compliant data changes (i.e. date, initials or signature with reason for change)]
- Definition of raw data
- Data integrity
- Archiving and restoring electronic data
- Electronic data ownership and access rights

6 ROLE OF TEST FACILITY QA

Before the test facility commits to the services of an external IT service provider, a supplier audit may be appropriate. Ideally, the audit team is multi-disciplinary (QA, IT, line function subject matter expert) to cover the scope of the provided service(s).

In this audit, the following items may be assessed (list is not exhaustive):

- Quality System of the provider
- Documentation process of the provided service(s)
- Experience and training of the involved provider personnel
- Confidentiality and security of the test facility information/data

Technical experts may evaluate other items during the audit:

- Competence with regard to the service(s)
- Premises and technology used

If an SLA (or contract) is envisioned, it is recommended that QA checks the draft SLA in order to make sure that all aspects of GLP compliance as mentioned in chapter 4 are covered.

The periodic review of existing SLAs and the possibility of supplier audits should be defined in the QA program of the test facility. The documentation at the test facility and at the external IT service provider's facility should be checked according to the provisions of the SLA.

7 GLP MONITORING AUTHORITIES

During inspections, GLP Monitoring authorities may review SLAs and corresponding documentation at the test facility in order to assess a system's GLP compliance. As such, the SLA should allow access to IT service provider records/documents in a timely manner.

8 RISKS AND CRITICAL ISSUES

The following aspects may be critical and should therefore be considered:

- Merger or acquisition of external IT service provider
- Technologies such as cloud computing which could impact data integrity
- Out of business, e.g. insolvency of external IT service provider (impact on running services / stored and archived data, backups)
- Security breach at the IT service provider (notification to the test facility)

9 REFERENCES

[1] Ordinance on Good Laboratory Practice of 18 May 2005 [RS 813.112.1] as last amended on 1 December 2012. (OGLP)

[2] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 1: OECD Principles on Good Laboratory Practice (as revised in 1997). Environment Directorate, OECD, Paris, 1998. (OECD)

[3] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 17: Advisory Document of the Working Group on Good Laboratory Practice. Application of GLP Principles to Computerised Systems. Environment Directorate, OECD, Paris, 2016. (OECD)

[4] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 15: Advisory Document of the Working Group on Good Laboratory Practice. Establishment and Control of Archives that Operate in Compliance with the Principles of GLP. ENV/JM/MONO(2007)10; Environment Directorate, OECD, Paris, 2007. (OECD)

[5] Working Group on Information Technology (AGIT): Good Laboratory Practice (GLP); Change Management and Risk Assessment of Validated Computerized Systems in a GLP Environment. (AGIT)

10 WORKING GROUP ON INFORMATION TECHNOLOGY

The Working Group on Information Technology (AGIT) was founded on 27 March 1998 with the objective of discussing relevant topics of Good Laboratory Practice (GLP) in the field of information technology between industry and the monitoring authorities.

The AGIT intends to set up guidelines based on legislative requirements and practical experience to support test facilities introducing information technology tools to computerised systems in practice. OECD GLP Advisory Document number 17 on the Application of the Principles of GLP to Computerised Systems is used as a basis for discussion.

The members of the AGIT are representatives of the Swiss GLP monitoring authorities (Olivier Depallens, Swiss Federal Office of Public Health; Elisabeth Klenke and Daniel Roth, Swissmedic, Swiss Agency for Therapeutic Products; Christoph Moor, Federal Office for the Environment), and invited experts from industry (Peter Esch, Novartis Pharma AG; Stephan Hassler, Innovative Environmental Sciences Ltd.; Silvio Albertini, F. Hoffmann-La Roche AG; Christine Wurz, Idorsia Pharmaceuticals Ltd.).

For the convenience of users, AGIT publications are available on the Swiss GLP website (see Good Laboratory Practice (GLP)). The Swiss GLP homepage also provides links and references to guidelines, laws and regulations, definitions etc.

AGIT Publications:

- Guidelines for the Validation of Computerised Systems
- Guidelines for the Management of Electronic SOPs in a GLP Environment
- Guidelines for the Archiving of Electronic Raw Data in a GLP Environment
- Guidelines for the Acquisition and Processing of Electronic Raw Data in a GLP Environment
- Guidelines for the Development and Validation of Spreadsheets
- Guidelines for Change Management and Risk Assessment of Validated Computerized Systems in a GLP Environment.
- Position Paper 1: Is it acceptable to destroy the paper originals of raw data and related study documentation, if an image of the paper is captured in an electronic form (e.g. scanned)?
- Guidelines for Collaboration with External IT Service Providers Supporting a GLP Environment