Good Laboratory Practice

GUIDELINES FOR THE ARCHIVING OF ELECTRONIC RAW DATA IN A GLP ENVIRONMENT

Release Date: 27.05.2026

Version: 3.0

TABLE OF CONTENTS

1 FOREWORD 3
2 INTRODUCTION 3
3 SCOPE 3
4 ELECTRONIC RAW DATA 4
4.1 Definition of Electronic Raw Data 4
4.2 Elements of Electronic Raw Data 4
5 ROLES AND RESPONSIBILITIES 5
5.1 Test Facility Management (TFM) 5
5.2 Study Director 5
5.3 Archivist / IT Personnel 5
5.4 Quality Assurance (QA) 6
6 ARCHIVING OF ELECTRONIC RAW DATA 6
6.1 Integrity of electronically archived data 6
6.2 Archiving possibilities 7
6.2.1 Offline archiving on a mobile storage medium 7
6.2.2 Online archiving on infrastructure controlled by the Test Facility 8
6.2.3 Online archiving on infrastructure provided by third parties 8
6.3 Archiving Process 9
6.3.1 Transfer of data to the electronic archive 9
6.3.2 Access to archived electronic raw data 9
6.3.3 Deletion of electronically archived data 10
7 OPERATION OF ELECTRONIC ARCHIVES 10
7.1 General requirements and procedures for operating electronic archives 10
7.2 Data integrity checks 11
7.3 Migration of archived electronic raw data 11
8 REFERENCES 14
9 WORKING GROUP ON INFORMATION TECHNOLOGY 15

1 FOREWORD

The aim of the present document is to provide guidance on the GLP-compliant archiving of electronic raw data. It will aid test facilities and promote the use of a common standard, but it should not be considered as a legal document. 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 the Archiving of Electronic Raw Data in a GLP Environment were issued as Version 1.0 in May 2003. This updated version (version 3.0) should be read in conjunction with the relevant OECD Documents, e.g., OECD Advisory Document No. 17 (including supplement 1) [3, 4], OECD Advisory Document No. 15 [5] and OECD Advisory Document No. 22 [6].

2 INTRODUCTION

Computerised systems are used throughout the entire data life cycle, including acquisition, processing, reporting, archiving, and retrieval. In accordance with the GLP Principles, raw data — including electronic raw data — should be archived to ensure traceability and accountability of non-clinical safety studies [2].

During the archiving period, the integrity of electronic raw data should be preserved in line with the ALCOA+ principles (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available) as well as with the requirements of OECD Advisory Document No. 22 [6]. Therefore, electronic archiving processes should be adequately addressed in a data integrity risk assessment to ensure that potential vulnerabilities are identified and mitigated. The systems used for archiving require formal validation, as outlined in OECD Advisory Document No. 17 [3], to demonstrate their suitability and reliability for long-term data preservation.

OECD Document No. 22 differentiates between *dynamic* and *static* data and states that *dynamic data* should be retained in a dynamic format, as an interaction with such data may be required during the archiving period.

The intention of these guidelines is to clarify important aspects of the archiving of electronic raw data in a GLP environment. They are based on the Swiss Ordinance on Good Laboratory Practice [1], the OECD Principles of GLP [2], and the relevant OECD Advisory Documents [3, 4, 5, 6]. This document should also be read together with the AGIT guidelines on the acquisition, processing, and storage of electronic raw data, which cover the steps in the data life cycle prior to archiving [7].

3 SCOPE

This document provides guidance on the archiving of electronic raw data in a GLP environment. It addresses the following aspects:

- Regulatory requirements for electronic archiving under GLP

- Different options for electronic archiving
- Integrity of archived electronic raw data, including measures to ensure authenticity, reliability, and protection against unauthorised access and changes
- Archiving process of electronic raw data
- Availability of electronic raw data during the entire retention period, ensuring timely retrieval for study reconstruction
- Operation of electronic archives, long-term considerations related to archiving, including strategies to maintain data accessibility and readability in line with GLP requirements

4 ELECTRONIC RAW DATA

4.1 Definition of Electronic Raw Data

Raw data are defined in the OECD Principles of GLP [2] as follows:

Raw data means all original test facility records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study. Raw data also may include, for example, photographs, microfilm or microfiche copies, computer readable media, dictated observations, recorded data from automated instruments, or any other data storage medium that has been recognised as capable of providing secure storage of information for a time period specified by the appropriate authorities (i.e., for a time period of at least ten years as required by the Swiss Ordinance on GLP [1]).

For the purpose of these guidelines, the definitions of the term electronic raw data and of its various forms are given below.

Electronic Raw Data:	Original records, or verified copies thereof, generated by means of computerised systems and stored on digital media. They are necessary for the evaluation and reconstruction of study results and may exist in a static or in a dynamic format as defined in OECD Advisory Document No. 22 [6].
Proprietary Form:	A file format, which needs a dedicated software to be read and processed.
Human Readable Form:	A file format that can be interpreted by standard software to view the content in human readable form as text, figures, graphs, tables, etc.

4.2 Elements of Electronic Raw Data

Electronic raw data consist of the data including the associated metadata. The data represent the core data elements (measured values), whereas metadata comprise the attributes of the measured values (e.g., study number, time, sample identification) and technical properties (e.g., field properties, table relationships, etc.). The processing of electronic raw data such as integration, calibration, and calculation should be documented including processing parameters, equations and statistical methods.

All changes to electronic raw data have to be recorded in an audit trail specifying the original and modified data, the reason for change, date and time, and the identity of the person making the change.

According to OECD Advisory Document No. 22 [6] retained records should allow reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported.

If there are electronic and paper-based data in a study, this should be described in an index. The link between the electronic raw data and the paper data should be described to ensure data integrity.

5 ROLES AND RESPONSIBILITIES

5.1 Test Facility Management (TFM)

The test facility management should designate an archivist and, where necessary, other personnel under the supervision of the archivist for the management of the electronic archive. Such personnel should be qualified and have appropriate training to perform their duties in accordance with the GLP Principles. If archiving services are obtained from external service providers, the TFM should ensure that these services are carried out in accordance with GLP, e.g., via Service Level Agreement [3, 4, 8].

The TFM should ensure that appropriate facilities, equipment, materials and SOPs are available for electronic archiving and that the electronic archiving systems are suitable for their intended purpose and are validated, operated and maintained in accordance with the Principles of GLP [2].

Furthermore, the TFM should consider the electronic archiving systems and all aspects of the life cycle of archived electronic raw data in the data governance framework of the test facility and ensure that there are no unacceptable risks to data integrity [6].

5.2 Study Director

The study director should ensure the proper archiving of all study data, including electronic raw data [2, 5]. The study director is responsible for verifying the integrity and establishing an index of all data transferred to the archive, including the electronic raw data.

5.3 Archivist / IT Personnel

The archivist is responsible for the archiving process, operation of the archives and maintenance of the integrity of archived data throughout the archiving period, including electronic archiving, and should exercise appropriate control over all related activities.

It may be necessary to delegate certain tasks to IT personnel. The collaboration between IT personnel and archivist should be defined, e.g., in an SOP. If there is external IT involvement (service provider), the archivist should ensure that the procedures defined in the relevant service level agreements or contracts are followed [5].

Interactions between the archivist, IT personnel and the study director involved at any stage of the archiving process should be documented.

5.4 Quality Assurance (QA)

The QA is responsible for inspecting all aspects of archiving for compliance with the GLP Principles. This includes the inspection of archiving procedures for electronic raw data and of the electronic archiving system including the IT-infrastructure, as well as archived study- and facility records, documents concerning the personnel and, if applicable, the activities of external service providers involved in electronic archiving.

The QA should be qualified in terms of IT knowledge and properly trained in the corresponding archive systems to be able to inspect electronic archiving procedures.

6 ARCHIVING OF ELECTRONIC RAW DATA

6.1 Integrity of electronically archived data

Requirements for the archiving of electronic records are the same as those for other record types as outlined in OECD Advisory Document No. 15 [5]. Archiving systems and archiving processes should be subject to a risk-based validation [3, 9].

All aspects of data integrity (ALCOA +) are relevant for archived electronic data, during the entire retention period which may include system retirement, as shown in the following examples:

- Attributable/Contemporaneous: The audit trail relevant for the reconstruction of the data generation should be available and linked to the records and system accordingly. Electronic signatures should be valid over the entire archiving period.
- Legible: Reconstruction of study results should be possible over the entire retention period. Measures should ensure the availability of adequate software solutions or other means to access the data; this may include timely data migration [3].
- Original/Accurate: The archived data must be an exact representation of the original records. Users should be limited to read-only access to the archived records. It should not be possible to modify or delete archived data before the end of the retention period. A risk assessment should take into account that there are no limitations on the system administrator’s privileges with respect to the use of a computer system - and to apply suitable risk control procedures (see OECD FAQ Good Laboratory Practice and Compliance Monitoring [10]).
- Complete: The archiving of electronic data should be complete - this may be facilitated by a list of files together with other information such as size, archiving date, etc. This may also support navigation of the data.
- Consistent: The information to evaluate consistency of the data should remain available. The link between data and metadata needs to be maintained throughout the archiving period. This also applies to audit trails and electronic signatures.
- Enduring: Electronic archives should be protected by adequate data security measures. Physical storage conditions should ensure protection from heat, humidity, electromagnetic radiation or other threats.
- Available: It should be possible to locate and access the data in a timely manner.

When archiving dynamic data, the dynamic nature should be preserved with the functions to interact with it (e.g., filtering or displaying data differently). Archiving of dynamic data in static format should be limited to exceptional cases (i.e. legacy systems).

Retention of dynamic data (images, electronic signatures, chromatograms, etc.) requires that the relevant software solution (or other means of accessing and processing the data) remains available. Any loss of information should be identified and the risk to the integrity of the data set should be assessed and documented.

6.2 Archiving possibilities

Multiple approaches exist for the archiving of electronic data. For the purposes of these guidelines, technical solutions are classified in two categories: online archiving and offline archiving. The responsibilities of both, test facilities and third parties, are also reflected within this context.

- Offline archiving refers to electronic data stored in a physical archive on media such as USB drives or CDs/DVDs. Accessing these data requires physical retrieval of the storage medium from the archive.
- Online archiving concerns electronic data that remain accessible via a network e.g., on a cloud-based system.

It is recognised that within a test facility a combination of these archiving scenarios may be used. The TFM is responsible for maintaining oversight of the different archiving approaches (including any paper-based archiving), ensuring data integrity, and maintaining appropriate documentation (e.g., in the SOPs, an overview document or as additional information in the CS inventory). It is highlighted that an overview, or a central summary document is particularly useful, when different scenarios are in use.

6.2.1 Offline archiving on a mobile storage medium

Electronic raw data may be stored on mobile data media (e.g., CD/DVD, USB stick, external hard drive) and archived in a GLP archive.

Several points should be considered for this way of archiving:

- The maintenance of the overall index may be challenging as data may be split across multiple storage devices.
- Amending procedures (e.g., adding documents) may be difficult.
- A retrieval from the archive is necessary for reading the data.
- Such an offline storage requires manual backup procedures.
- Care must be taken to ensure that data formats and physical media do not become obsolete; if necessary, migrations must be carried out.
- Data migration would require additional manual data transfer steps.
- Physical performance of the storage media needs to be ensured, and regular medium refresh may be necessary (e.g., magnetic tape, CD/DVD).
- Mobile media such as USB sticks can be quite small and may get lost.

6.2.2 Online archiving on infrastructure controlled by the Test Facility

Online archiving can be achieved either by transferring the data to a dedicated electronic archive or by maintaining it on the original productive system, in which the archived electronic raw data are explicitly marked and locked. Both options allow that historical electronic data are directly accessible for further evaluation purposes.

If the data are kept in the productive system, the data integrity risk assessment should pay particular attention to the operation of the system including changes, maintenance. Procedures/measures should be in place to ensure that the archivist obtains full control over data integrity after the status is changed to archived.

Facility related processes should preserve data integrity, for example:

- Physical access management (allow, control, monitor, review access).
- Environmental conditions monitoring and protection (e.g., temperature, humidity, dust, flooding), fire protection or other risks.
- Secure electrical supply (potentially backup systems).

From a logical point of view, measures to ensure data integrity should also include:

- Logical access management (allow, control, monitor, review access), including administrators (restricted number).
- Backup and restoration (e.g., ensuring off-site backups).
- Change management process (e.g., new releases, maintenance), ensuring that archived raw data are not impacted and still retrievable and legible. When archived data are stored in a productive system, all changes to the productive system need to be assessed. This may result in more changes than for a dedicated archive system.

The requirements for archiving systems with respect to physical access to the system, restricted numbers of system administrators, system maintenance, and data protection are more readily met by using a dedicated electronic archive system.

In case of online archiving, it has to be ensured that the storage locations fulfil the requirements for a GLP archive. It is recommended that backups of archived electronic raw data be kept off-site under suitable conditions.

In addition, it is important to preserve historical results and report formats, including company name, department names, usernames, etc.

6.2.3 Online archiving on infrastructure provided by third parties

Where third parties are involved and responsibilities are distributed, the mechanisms for implementing and verifying requirements may differ. Nevertheless, the online archiving requirements specified in Section 6.2.2 remain applicable, as they address data integrity and data retrievability.

The roles and responsibilities for the service provided vary, in relation to the scope of the provided services: for example in a Software as a Service Archiving Application, the infrastructure, the application and the data are managed by the supplier, while for an in-house application hosted on a cloud infrastructure (Infrastructure as a Service), the application, data (and related processes such as backups, for example) are

managed by the Test Facility while the hardware and physical conditions are managed by the supplier [4].

Although the archive is not under direct control of the test facility, it should be ensured that the physical conditions (infrastructure, location) are suitable for archives. Logical measures should also be verified, including backup/mirroring and restoration processes. This may be done by auditing the supplier or its certifications and ensuring that a suitable Service Level Agreement (SLA) is in place. An SLA is key to ensure proper definition of roles and responsibilities, processes (including operation and maintenance), escalation procedures and communication (see OECD Document No. 17, supplement 1 [4], and AGIT Guidelines for Collaboration with External IT Service Providers Supporting a GLP Environment [8]).

This includes data-loss management, change management, and access management, which is subject to the oversight of the archivist.

Location of data should be defined/considered (e.g., legal aspects such as national laws in the country where the server is located). The ability of the supplier to provide the service over the entire retention period should be evaluated (regarding technical and financial aspects). It should also be ensured that an exit process is defined which includes all data that may have to be migrated.

Subcontractors (for example cloud service providers) may also be inspected for GLP compliance by monitoring authorities.

6.3 Archiving Process

6.3.1 Transfer of data to the electronic archive

For each study, the study director is responsible that all study related records are archived during or immediately after completion of a study.

There should be a validated process for the transfer of electronic raw data to the archive which ensures that data integrity is preserved.

In case of physical separation of the electronic archive (offline archive or productive and archiving system separated) the electronic raw data should be moved from the productive system to the archive destination and modification should not be possible anymore.

In case of logical separation of the electronic archive (data remain on the productive system) the electronic raw data should be set to read-only and clearly identified as archived.

Whichever archiving solution is selected, study documentation should have a complete index listing the electronic raw data and storage location. The administration of this index should be described in an SOP. With archiving, the archivist takes over the responsibility for the integrity of the data. The archivist should acknowledge the receipt of the data.

6.3.2 Access to archived electronic raw data

Electronically archived data need to remain available during the entire archiving period (e.g., for audits and inspections carried out by the authorities or by the QA). Electronic raw data and associated audit trails should be retrievable and made available in a human-readable format in a timely manner. For electronic data stored offline on mobile

storage media in a physical archive, the requirements for the retrieval procedures are the same as for paper-based records. Measures should be in place to prevent alteration or deletion of the data on the media and upon return a verification by the archivist is required, showing that the records are complete and unaltered. For data stored on electronic archives which are accessible remotely (e.g., on servers, cloud-based services), retrieval of the files is normally not required as read-only access can be granted (see OECD Document No. 15 [5]).

Regulatory and/or internal requirements can make further data processing/interpretation necessary. Re-opening of studies to add additional data or conduct additional data analysis should however occur only in exceptional circumstances (see OECD Document No. 21 [11]). Further processing of archived data should be subject to an authorisation procedure and a retrieval via archivist is necessary. If further data processing takes place, the original data should remain available and unchanged. All data generated during such a process should be archived in addition to the original raw data.

6.3.3 Deletion of electronically archived data

The process of deleting electronically archived data should be described in an SOP. Disposal of electronically archived data requires approval by the TFM and, if applicable, by the sponsor (see OECD Document No. 15 [5]). It is recommended that the archivist notifies the TFM after the defined retention period, which is at least 10 years according to the Swiss GLP Ordinance [1]. The retention period in other countries may differ. The decision by the TFM to dispose the archived data and the reason for their disposal should be documented.

7 OPERATION OF ELECTRONIC ARCHIVES

7.1 General requirements and procedures for operating electronic archives

Electronic archives should be operated in a way that data integrity is maintained throughout the entire archiving period.

It is expected that the procedures related to the operation of electronic archives are defined in an SOP and the activities conducted are documented. A description of the archiving sites, the systems in place, and the roles and responsibilities for the operation should be maintained and kept up to date.

The general procedures for the operation of electronic archives are comparable to those for the operation of other computerised systems. The following aspects should be considered:

- Physical security procedures: Servers or other storage media for electronically archived data as well as related data centres need to be designed, operated and maintained in a way that early deterioration of the records is prevented (see OECD Doc. No 17, Section 3.7 and further provisions in OECD Docs. No. 15 and 25 [3, 5, 12]).
- Data security procedures: Documented data security procedures should be in place to protect electronically archived data from unauthorised access, alteration or loss (see OECD Doc. No. 17, Section 3.7 and further provisions in OECD Docs. No. 15 and 25 [3, 5, 12]).

- Access rights: Access rights and user privileges for electronic archives should be assigned according to defined procedures, documented and updated when organisational changes occur. Potential conflicts of interest should be considered (see OECD Docs. No. 15, 17 and 25 [3, 5, 12]).
- Backup and restore procedures: Backup procedures should be available for electronically archived data. Backup procedures shall be tested with regard to data integrity (OECD Docs. No. 17 and 25 [3, 12]).
- Incident Management: Any incidents which occur to the archiving systems during operation and any actions taken in response should be documented, assessed, particularly also regarding the integrity of the archived data. (OECD Doc. No. 17, section 3.8 [3]).
- Disaster recovery: Plans for the recovery of archived data and/or system in case of system failure should be available (see OECD Doc. No. 17, section 3.12 and general provisions in OECD Doc. No. 15 [3, 5])
- Change management: Any changes to the archiving procedures and/or archiving system should follow change control procedures which encompass an assessment of the risks associated with the change. Depending on the outcome of the risk assessment, additional validation activities of the system may be required (see OECD Doc. No. 17, Section 3.5 and AGIT Guidelines on Change Management [3, 13]).

Archiving systems for electronic data should be subject to a periodic review to ensure that they remain fit for their purpose (see OECD Doc. No. 17, section 3.6 [3]).

7.2 Data integrity checks

The integrity of the archived data should be checked at appropriate intervals and documented including any follow-up actions. Checks can be conducted with a representative sample of archived data and should verify at least the following points:

- The archived records can be opened with the relevant software and have maintained their dynamic attributes (e.g., interaction with the data is still possible).
- Completeness of the data (e.g., match the index).
- The associated metadata are available and correctly linked to the archived records.
- Electronic signatures are still valid and attributable.

The frequency of data integrity checks should be based on a risk assessment and documented. The same considerations apply to the backups of the data.

7.3 Migration of archived electronic raw data

Data migration is the process of moving electronic data between different data storage types, computerised systems, or simply the transition of data from one format to another. This may include changing the format of data, but not the content or meaning, to make it usable or visible on an alternative computerised system (OECD Document No. 22 [6]).

Migration of electronically archived data becomes necessary when the long-term availability, readability, or integrity of the records can no longer be ensured within the existing environment.

Typical situations requiring data migration in the context of electronic archiving include:

- Same system migration (e.g., refresh of the storage medium, transfer from one server to another)
- Migration to another archiving system (e.g., due to change of cloud service provider)
- Migration to a different data format (e.g., due to upgrade or retirement of the system required to read the archived data)

Data migration efforts may vary greatly in complexity and risks (see OECD Document No. 17 [3]). Data migration may consist of a copying process, or it may require complex procedures including the development of software or approaches to interpret the data structure of the legacy system and convert them to the format of the new system.

Data migration should preserve all aspects of data integrity including completeness (with all metadata), accuracy and legibility.

The risks to data integrity associated with the migration process should be systematically assessed, and the migration approach should be designed to minimise these risks. The data migration process should be validated.

Migrating data can involve a format change, and is generally done step by step, each bringing specific risks. Additionally, a migration may be partial (i.e., only selecting some data) or total (e.g., when the whole system is to be decommissioned). To mitigate the risks, it is key to define controls for each step, final controls and ensuring that the process is tested.

Once the source and the target system (and/or formats) are defined the following stepwise approach can be applied for the migration:

Step	Description	Point to consider
Scope definition	Defining which data are to be migrated.	Ensure that all relevant data are in the scope of the migration (e.g. metadata, audit trail information).
Mapping	Detailed planning of transformation from source to target.	Define how each part of the data in the source system (e.g. field in the database) will be stored in the target system. Determine how the data will be transferred to the target system and if transformation of the data is necessary. Data may need to be split or merged (depending on field lengths and formats), and empty data fields may need to be

		populated with default/neutral values.
Extraction	Extracting the data defined in scope	Ensure controls are in place to compare the extracted data against the data in the source system (e.g. by counting the records).
Transformation	Transforming the extracted data as defined in the mapping.	Ensure that the transformation steps are properly executed (e.g. by a detailed check of a representative sample).
Upload to target system	Upload the extracted and transformed data into the target system.	Ensure that the transferred data are legible and retrievable and complete (including previous audit trails and signatures). Ensure that all data in scope have been uploaded.

According to OECD Document No. 17 [3], data migration should be part of the test facility management's validation scope. The scoping and mapping can be considered analogous to the user requirement specifications in a computerised system validation. There should be a migration plan, testing against the requirements (may be iterative), execution, verification and reporting and release/approval of the migrated data.

8 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 of Good Laboratory Practice* (as revised in 1997), OECD Publishing, 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.* OECD Publishing, Paris, 2016. (OECD)

[4] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No 17 Supplement 1: *Advisory Document on GLP & Cloud Computing,* OECD Publishing, Paris, 2023. (OECD)

[5] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 15: *Advisory Document of the Working Group on GLP: Establishment and Control of Archives that Operate in Compliance with the Principles of GLP*, OECD Publishing Paris 2007. (OECD)

[6] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 22: *Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity*, OECD Publishing, Paris, 2021. (OECD)

[7] Working Group on Information Technology (AGIT): *Guidelines for the Acquisition and Processing of Electronic Raw Data.* (AGIT)

[8] Working Group on Information Technology (AGIT): *Guidelines for Collaboration with External IT Service Providers Supporting a GLP Environment.* (AGIT)

[9] Working Group on Information Technology (AGIT): *Good Laboratory Practice (GLP); Guidelines for the Validation of Computerised Systems.* (AGIT)

[10] OECD Good Laboratory Practice: *Frequently Asked Questions (FAQ)*, accessed on 18.05.2026. (OECD)

[11] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 19: *Position Paper Regarding Possible Influence of Sponsors on Conclusions of GLP Studies*, Paris, 2020. (OECD)

[12] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 25: *Position Paper on Good Laboratory Practice and IT Security*, OECD Publishing, Paris, 2024. (OECD)

[13] Working Group on Information Technology (AGIT): *Guidelines for Change Management and Risk Assessment of Validated Computerised Systems in a GLP Environment.* (AGIT)

9 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 list of the current members of the AGIT (i.e., invited experts from industry and representatives from the Swiss GLP monitoring authorities) is available in the AGIT section on the Swiss Good Laboratory Practice (GLP) website.

The AGIT provides guidelines based on legislative requirements and practical experience to support test facilities in applying the GLP Principles to information technology. AGIT publications are available on the Swiss Good Laboratory Practice (GLP) website (AGIT section).