chemgineering

MOLECULAR DEVICES

SYSTEM ASSESSMENT REPORT

"Electronic Records, Electronic Signatures" regarding 21 CFR Part 11[1] / EU GMP Annex 11[2]

System: **SoftMax Pro GxP[3]** Version: **7.1**

Interviewer / Author	Peter Berger, Sieghard Wagner
Date of Interview	11-Apr-2019

[1] see CFR - Code of Federal Regulations Title 21, https://www.fda.gov
[2] see EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines, https://ec.europa.eu/health/documents/eudralex/vol-4_en
[3] The label „SoftMax Pro GxP" comprises of the four software components "GxP Admin", "SQL-Database", SoftMax Pro" and "GxP Admin Portal"

Chemgineering Austria GmbH, EURO PLAZA 2E, Technologiestraße 10 / 2. OG, 1120 Wien, Tel.: +43 1 25574 1339

Content

0 General System Information

0.1 GxP - Processes

Does the system support GxP-relevant processes?

☒ **Yes**[4] / ☐ **No**

Justification / Processes names:

The answer to this question depends on the application of SoftMax Pro GxP, and has to be given by the respective process owner of the customer. The process owner has the knowledge about the business process, its GxP relevance and the GxP impact of SoftMax Pro GxP on this process.

0.2 Electronic Records (Section 1)

Is the system used to manage (create, manipulate, administer, re-store, transmit or archive) electronic records?

☒ **Yes**[4] / ☐ **No**

The answer to this question depends on the application of SoftMax Pro GxP, and has to be given by the respective process owner of the customer. That person has the knowledge about the types of electronic records the software has to manage.

Describe the nature / type / purpose of the electronic records?

SoftMax Pro GxP basically manipulates 2 types of data. The “Protocol” and the “Data Document”. Whereas the “Protocol” defines the method for data capture and analysis, the “Data Document” comprises samples, raw data and results of calculations.

0.3 Closed System / Open System (Section 2)

Is the computerised system a closed or open system?

☒ **Closed system** ☐ **Open system (Section 2)**

SoftMax Pro GxP infrastructure components are connected using WAN/LAN and the data flow only stays within this boundaries. Data transfer via the Internet is not intended.

[4] For the purpose of this ERES assessment, it is assumed that SoftMax Pro GxP supports GxP processes, including processing of electronic records.

0.4 Hybrid System (Section 3)

Is a printout of the e-record signed on paper and used instead of the electronic original?

☒ **Yes** / ☐ **No**

SoftMax Pro GxP offers the functionality for operation as a hybrid system, but the actual answer depends on the application of SoftMax Pro GxP, and has to be given by the respective process owner.

0.5 Electronic Signatures (Section. 3 to 7)

Are electronic signatures used and serve as equivalent to paper based signatures?

What type of documents are signed electronically?

☒ **Yes** / ☐ **No**

It is possible to sign “Protocols” and “Data Documents” electronically by means of SoftMax Pro GxP.

1 Procedures and Controls for Closed Systems

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
1	11.10 (a) A11: Principle A11:1 A11:2 A11:3 A11:4	Validation, IQ, OQ	Is the system validated?	**O**		The process owner/operator is solely responsible for the validation of the system. The responsibility of the supplier lies in supplying systems, which are capable of being validated. This is supported by the internal quality management system, of Molecular Devices, which can be audited on request. Molecular Devices runs a certified quality management system based on the requirements of ISO 9001:2015. Molecular Devices also offers a range of validation services: Conformity certificates, prepared documentation for IQ and OQ as well as performing IQ and OQ at the operator's premises.
2	11.10 (a) A11:8.2 A11:9	Audit Trail, Change	Is it possible to discern invalid or altered records?	**X**		During processing a status of "Cancelled" is applied to records to mark them as obsolete. SoftMax Pro GxP has implemented diverse plausibility checks, and so invalid data are recognized and capturing of such is prohibited automatically. Changes to records are documented within the audit trail. In case of any data import a checksum is used to detect inconsistencies. Such records will not be imported and in addition the user is informed via a report.

[5] Reference to the 21 CFR Part 11 ('11.nn') and/or EU GMP Guidelines Annex 11 ('A11:…') paragraphs;
The following Annex 11 paragraphs are not referenced since they apply definitely to the operator only: A11:11 "Periodic Evaluation", A11:13 "Incident Management", A11:15 "Batch Release" and A11:16 "Business Continuity"
[6] see: Good Practice and Compliance for Electronic Records and Signatures Part 2, Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures; A document produced jointly by ISPE and PDA

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
3	11.10 (b) A11:8	Report, Printout, Electronic Record	Is the system capable of producing accurate and complete copies of electronic records on paper?	**X**		The system allows to print electronic records (“Protocol” and “Data Document” information) on paper formatted as report. Users are able to configure these reports, in case they have required permissions (role concept). The content for these reports is configurable (via checkboxes).
4	11.10 (b)	Report, Electronic Record, FDA	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	**X**		The system allows to print electronic records (“Protocol” and “Data Document” information) to PDF[7] format or they can be provided as signed XML[8] files.
5	11.10 (c) A11:7.1 A11:7.2 A11:17	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	**X/O**		The system owner/operator is solely responsible for record storage/archiving. SoftMax Pro GxP keeps all data which are relevant for operation inside the system and as long as wished. The current version 7.1 provides a function for data import, including version 4.0 or younger of SoftMax Pro GxP. As „Protocol“ and „Data Document“ information are regarded as static, it is possible to archive them in PDF format.

[7] PDF: Portable Document Format
[8] XML: Extensible Markup Language

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
6	11.10 (d) A11:12	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals? Are creations or modifications of roles and access rights recorded?	X		SoftMax Pro GxP offers a role-based user permissions concept. A user takes a role (assigned by the systems admin) and permissions of that role are passed on to that person. In a next step user are added to projects and assigned a role .The system ensures that a certain user cannot take more than a single role in that particular project. It is possible to manage system users via the active directory to verify their identity. All changes regarding system roles (creation, change, deletion) are recorded in the audit trail. All allocations and changes of user access rights (creation, modification or rejection) are recorded in the audit trail.

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
7	11.10 (e) A11:9 A11:12.4	Audit Trail, Electronic Record, Operator Entries	Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records? Does the audit trail (mandatorily) collect the reason for a record change or deletion?	**X/O**		All changes to “Protocols” or “Data Documents” (creation, change, deletion) are recorded in the systems audit trail. The audit trail includes: - A time stamp (UTC[9] + local time) - User ID - Event Type (login, change, data acquisition, settings) - Data (old value, new value) - Document Name - Software version - Computer / workstation name. The server’s time is used to generate the time stamp of the applications audit trail. The reliability of this time source is crucial and has to be verified by the process owner/operator during the systems validation. For certain changes to records a mandatory comment is enforced (Excluding of analysis data / Setting the "Released" status / Signing of Statements). Comments going beyond this must be organized by the operator. The audit trail allows the authorized user to add comments. The audit trail is saved to a database und secured with the same methods as the database itself.

[9] UTC: Temps Universel Coordonné (French for ‚Coordinated Universal Time‘)

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
8	11.10 (e)	Electronic Record, Overwriting data, Change	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?	**X**		Upon changes of records an entry in the audit trail is made. The old and new value are logged. The systems workflow enforces that “Protocols” have to be saved using the “Save As” function. That ensures that new versions are generated and recorded within the audit trail.
9	11.10 (e) A11:7.1	Audit Trail, Retention Period	Is the audit trail of an electronic record retrievable throughout the retention period of the respective record?	**X/O**		SoftMax Pro GxP keeps all data inside the system as long as wished. All data (including audit trail) are saved to a database and so data consistency is achieved. It is up to the process/data owner to ensure correct backup and archival are properly executed and to verify that access is possible throughout the retention period.
10	11.10 (e)	Audit Trail, FDA, Inspection	Is the audit trail available for review and copying by the FDA?	**X**		It is possible to print stored data to PDF and make printouts as well as to provide this information as signed XML file; electronically or in paper format. The system offers the possibility to set up a role with access to the audit trail only.
11	11.10 (f)	Control over sequence of steps, Plausibility Check, Devices	If the sequence of system steps or events is important, is this enforced by the system (e.g., as it would be the case in a process control system)?	**X**		A workflow can be defined and so enforce a specific sequence of activities throughout the data capture process. For data capture the system works according predefined methods (as defined in the “Protocol”).

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
12	11.10 (g) A11:12.1	Login, Access Protection, Authorization, User, Administrator	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?	X		SoftMax Pro GxP offers a role-based user permissions concept. A user takes a role (assigned by the systems admin) and permissions of that role are passed on to that person. In a next step roles are assigned to projects and the system ensures that a certain user cannot take more than a single role in that particular project. It is possible to use the Active Directory for a central management of the user's credentials. All changes regarding system roles (creation, change, deletion) are recorded in the audit trail. All allocations and changes of user access rights (creation, modification or rejection) are recorded in the audit trail. The system ensures that a user can sign a single record just once. A user account can only be deactivated but not be deleted and the system makes sure that user IDs are unique.
13	11.10 (h)	Balance, Connection, Terminals, Input data, Devices	Does the system control validity of the connected devices? *If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g., terminals) does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).*	X		SoftMax Pro GxP connects only to known devices which are developed and built by Molecular Devices. Within the "Protocol" the required devices are specified and SoftMax Pro GxP recognizes if a wrong appliance is joint. Data from external capturing devices can only be imported to SoftMax Pro GxP and are marked with the attribute „imported".

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
14	11.10 (i) A11:2	Training, Support, User, Administrator	Is there documented training, including on the job training for system users, developers, IT support staff?	**X/O**		All personnel of Molecular Devices are trained according to their roles. This requirement is part of the internal quality management system (QMS) and includes GxP training. It is up to the process owner's organization to implement appropriate training for system users, administrators and IT staff.
15	11.10 (j) A11:14a	Policy, Responsibility, Electronic Signature, Signature Impact	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures? Does the electronic signature have the same impact as the handwritten signature?	**O**		It is up to the process owner's organization to implement appropriate training and awareness about the meaning of electronic signatures.
16	11.10 (k)	Documentation, Distribution of Documentation, Access to Documentation, System Documentation, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	**X/O**		SoftMax Pro GxP is delivered including user documentation which can be accessed directly through the system. Context related help information is available as well. It is up to the process owner to control and distribute appropriate operating manuals and release notes to personnel.
17	11.10 (k) A11:4.2 (A11:10)	SOP, Documentation, Manuals, System Documentation, Audit Trail , Logbook	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail (= version history) for creation and modification?	**X/O**		User documentation (release notes, user guide, installation guides etc.) is being controlled by Molecular Devices, including version control information. Once delivered the control responsibility is with the customer.
18	A11:6	Manual Data Entry , Electronic Record, Operator Entries	Are there checks to verify critical data entered manually?	**X**		The system allows assay specific configuration of plausibility checks like ranges, data types and nomenclature.

ID	Ref.[5]	Topic	Question[6]	Yes	No	Comments
19	A11:4.8	Data Migration , Electronic Record	Are electronic data to be migrated from one system instance to another are checked for consistency (e.g. no change of values or meaning)?	X		Data migration and import use a checksum to verify correct data transfer. So inconsistencies are detected and import to a target system is prohibited. All system changes, including those that can lead to change or values, are recorded in the release notes.

2 Additional Procedures and Controls for Open Systems

ID	Ref.[5]	Topic	Question	Yes	No	Comments
20	11.30 A11:5	Data, Encryption, Data Transfer	Is the data integrity of the electronic records protected, when they are process via the internet? Is data encrypted?	N/A		SoftMax Pro GxP is installed and configured as a closed system.
21	11.30 A11:5	Electronic Signature	Are digital signatures used to authenticate the involved parties?	N/A		SoftMax Pro GxP is installed and configured as a closed system.

3 Signed Electronic Records

ID	Ref.[5]	Topic	Question	Yes	No	Comments
22	11.50 A11:14c	Electronic Signature	Do signed electronic records contain the following related information: - The printed name of signer, - The date and time of signing, - The meaning of the signing (such as approval, review, responsibility)?	X		SoftMax Pro GxP electronic signature includes: ▪ User ID and name (additionally the full name is captured via user management and the name is included within the audit trail); ▪ Date and time; ▪ When configuring fields for signatures the meaning of the signature can be added; ▪ A mandatory field for comments can be used to document the meaning of the signature.
23	11.50	Electronic Signature	Is the above information shown on displayed and printed copies of the electronic record?	X		Electronic signature information is included in printouts. Within the system electronic signatures can be found under the menu item „Statements“.
24	11.70 A11:14b	Electronic Signature	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	X		The system does not provide a function to access or alter electronic signatures. All data are stored in a proprietary format and encrypted.

4 Electronic Signatures (General)

ID	Ref.[5]	Topic	Question	Yes	No	Comments
25	11.100 (a)	Electronic Signature	Are electronic signatures unique to an individual?	X		Within SoftMax Pro GxP electronic signatures are linked to user IDs and the system ensures that user IDs are unique.

ID	Ref.[5]	Topic	Question	Yes	No	Comments
26	11.100 (a)	Electronic Signature	Does the system prohibit that electronic signatures are ever re-used by, or reassigned to, any-one else?	**X/O**		Within SoftMax Pro GxP electronic signatures are linked to user IDs and the system ensures that user IDs are unique. It is up to the process owner's organization to implement a procedure for identification and user management. Users can't be deleted, only inactivated.
27	11.100 (a)	Electronic Signature, Representative	Does the system allow the trans-fer of the authorization for elec-tronic signatures (to representa-tives)?	**X/O**		Substitution rules within the system can be configured via the concept of system roles. This ensures that it is always clear who signed a record electronically. It is up to the process owner to ensure substitution rules for signing records electronically.
28	11.100 (b)	Electronic Signature	Is the identity of an individual verified before an electronic sig-nature is assigned?	**O**		The system offers the function for electronic signatures only to individuals who are logged in by using user ID and password. It is up to the process owner's organization to implement a procedure for identification and user management.

5 Electronic Signatures (Non-Biometric)

ID	Ref.[5]	Topic	Question	Yes	No	Comments
29	11.200 (a) (1)(i)	Electronic Signature	Is the signature made up of at least two components, such as an identification code and pass-word, or an ID card and pass-word?	**X**		To get system access a unique combination of user ID and password is required.

ID	Ref.[5]	Topic	Question	Yes	No	Comments
30	11.200 (a) (1)(ii)	Electronic Signature	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session).	**X**		Under all circumstances an electronic signature always requires the entry of user ID and password from a user who is already logged in to the system.
31	11.200 (a) (1)(iii)	Electronic Signature, Representative	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	**X**		Under all circumstances an electronic signature always requires the entry of user ID and password from a user who is already logged in to the system.
32	11.200 (a) (2)	Electronic Signature	Are non-biometric signatures used by their genuine owners only?	**O**		It is up to the system owner's organization to implement a procedure for user identification and management.
33	11.200 (a) (3)	Electronic Signature	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	**X/O**		No user/administrator has access to the electronic signature data by ordinary means. Only system administrators are able to reset a password and then misuse it for an electronic signature. But such fraud would be documented in the audit trail and could be traced back to that person. The system does not allow users to modify any meta data. It is up to the process owner's organization to implement appropriate training for system users and system administrators.

6 Electronic Signatures (Biometric)

ID	Ref.[5]	Topic	Question	Yes	No	Comments
34	11.200 (b)	Electronic Signature, Biometric Electronic Signature	Has it been shown that biometric electronic signatures can be used by their genuine owner only?	N/A		SoftMax Pro GxP does not offer the functionality of biometric signatures.

7 Controls for Identification Codes and Passwords

ID	Ref.[5]	Topic	Question	Yes	No	Comments
35	11.300 (a)	Identification Code, Uniqueness, Password, Identification, Login, Access Protection	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	X		The system controls the uniqueness of user IDs via GUIDs[10]. It is up to the process owner's organization to control the relationship of user ID to a person (see 28).
36	11.300 (b)	Identification Code, Password, Validity, Identification, Login, Access Protection	Are procedures in place to ensure that the validity of an identification code is periodically checked?	X/O		According to system configuration passwords have to be altered after a certain period of time. The system can be connected to the company Active Directory system. It is up to the system owner to implement a procedure for user and password management.

[10] A universally unique identifier (UUID) is a 128-bit number used to identify information in computer systems [Wikipedia]

ID	Ref.[5]	Topic	Question	Yes	No	Comments
37	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	X/O		According to system configuration passwords alter and have to be changed after a certain period of time. The system can be connected to the company Active Directory system. It is up to the system owner to implement a procedure for password management.
38	11.300 (b)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	X/O		User IDs can be deactivated within the system by the system administrator, but cannot never be deleted. It is up to the system owner to implement a procedure for user and password management.
39	11.300 (c)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection, Loss of ID card	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	X/O		User IDs can be deactivated by the system administrator. It is up to the system owner to implement a procedure for user and password management.
40	11.300 (c)	Loss of / compromised ID card, Electronically Disabling ID card	Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?	N/A		There are no hardware token or devices for user identification implemented.
41	11.300 (c)	ID card, Replacement	Are there controls over the temporary or permanent replacement of a device?	N/A		There are no hardware token or devices for user identification implemented.

ID	Ref.[5]	Topic	Question	Yes	No	Comments
42	11.300 (d)	Unauthorized Use, Login, Access Protection	Are there security safeguards in place to prevent and/or detect attempts of unauthorized use of user identification or password?	X/O		According to system configuration a user account is locked after a certain number of unsuccessful login attempts. In case a user account has been locked an entry to the admin dashboard and the audit trail is made. It is up to the system owner to implement a procedure for user account management and reopening a locked account.
43	11.300 (d)	Unauthorized Use, Login, Access Protection, Inform management	Is there a procedure in place to inform the responsible management about unauthorized use of user identification or password?	X/O		In case a user account has been locked an entry to the admin dashboard and the audit trail is made. It is up to the system owner to implement a procedure for system security including reporting responsibilities.
44	11.300 (e)	Testing of ID cards, ID card, Access Protection	Is there initial and periodic testing of tokens and cards?	N/A		There are no hardware token or devices for user identification implemented.
45	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does the token or card testing verifies that there have been no unauthorized alterations?	N/A		There are no hardware token or devices for user identification implemented.

Legend

X Applies to system
O Implementation is in the operator's responsibility
N/A Not applicable to the system

This 21 CFR Part 11 assessment is based on answers received during the workshop at Molecular Devices performed on April 11, 2019. Subject of this audit was the system SoftMax Pro GxP version 7.1 with all compliance features enabled.