UNIVERSAL AMENDMENT TO STANDARD CONTRACT FOR MICROSOFT AZURE/APPSOURCE MARKETPLACE

Version 01_04_23

This Amendment adds and modifies the corresponding provisions of the Microsoft "Standard Contract" (version March 2019) for the YSoft Clerbo solution as offered in the Microsoft Azure Marketplace for the following sections:

Section 11.10 Miscellaneous
Replaced in its entirety with the following text:

"This Agreement is governed by the laws of the Czech Republic and all disputes arising from, and in relation to, this Agreement shall be resolved with final effect by the competent court of the Publisher."

In accordance with Section 4, the Publisher will grant the SLA as set out in the relevant SLA description, available at legal section of the Microsoft Azure Marketplace from time to time or as otherwise communicated to Customer in the future.

Section 8(d)
Replaced in its entirety with the following text:
"Exceptions. No limitation or exclusions will apply to liability arising out of either party's: (1) confidentiality obligations under Section 3; (2) defense obligation under Section 7; (3) violation of the other party's intellectual property rights; (4) gross negligence, willful misconduct, or fraud; ***or (5) liability stemming from breach of Publisher's obligations vis-à-vis personal data processing.****"*

Section 12 Definitions
Definition of Offering is as follows:
*""**Offering**" means all services, websites (including hosting), solutions, platforms, and products identified in an Order and that Publisher makes available under or in relation to this Agreement, including the software, equipment, technology, and services necessary for Publisher to provide the foregoing. Offering availability may vary by region.* ***For avoidance of doubt, any professional services, such as implementation services and similar, are not a part of anz Offering, unless expressly agreed otherwise. The Publisher will be obliged to provide any professional services only subject to its express consent and a valid statement of work signed by Publisher and you, in place.****"*

Change and modifications.
The Publisher may, at its sole discretion and without any liability to you, modify, suspend or discontinue all or any part of the SaaS Offering provided to you, including its features, functionality, user interface, and third-party integrations, at any time and without prior notice.

However, the Publisher shall use reasonable efforts to notify you of any material adverse changes in the Offering that may substantially affect your use of the service, such as the removal of key features, a significant decrease in service level, or a change in pricing. Such notice may be provided via email, in-product messaging, or any other means deemed appropriate by the Publisher.

You acknowledge and agree that the Publisher shall have no obligation to maintain or provide any support or upgrades for the Offering, unless otherwise agreed upon in writing between the parties. The Publisher may also impose reasonable limits on the use of the Offering, such as storage capacity, bandwidth usage, or number of users, and may modify such limits from time to time, subject to prior notice to you.

You further acknowledge and agree that the Publisher shall not be liable to you or any third party for any modification, suspension, or discontinuance of the Offering, or any part thereof, except as expressly provided in this agreement or as required by applicable law.

By using the SaaS Offering, you agree to be bound by this clause and to regularly check for any updates or changes to it. If you do not agree with any modification, suspension, or discontinuance of the Offering, your sole remedy shall be to terminate this agreement and cease using the service.

ANNEX 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

NOT USED

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller: Customer using the YSoft Clerbo application operated and managed in Microsoft Azure by the Processor

Processor:

Y Soft Corporation, a.s., with registered office at Technická 2948/13, 61600 Brno, ID No.: 26197740, VAT No.: CZ26197740, file No. B 8045, registered with the Regional Court in Brno

Processor appointed the Data Protection Officer, accesible at dpo@ysoft.com

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

1. Data subjects are natural persons – users of YSoft Clerbo, for whom the Controller creates a user profile will be created by the Administrator in the application, i.e. usually employees or persons in a similar position in relation to the Administrator.

Categories of personal data processed

1. User identification data contained in each user's user profile. Depends on the specific settings of the user profile content with the administrator. It will usually include first name, last name, email address, organizational classification, role, photo. Identification data is processed in a structured form that allows it to be automatically retrieved and changed at the database level.
2. Content data. Content data consists of all content that a user creates and places in the system under his/her user profile. Depending on its nature, content data can be processed in structured form or as unstructured attachments in the form of video or photographs. Content data in structured form can be searched and further edited automatically, while unstructured data may require manual control depending on their nature and it is advisable to regulate their placement in the application by an internal regulation that sets out the rules for the placement of personal data in the form of unstructured data in the application.
3. Audit log. An audit log is a record in a database containing data about the user's use of the system. It contains the User ID - a pseudonymized identifier of the user and logs of the user's actions in the system. The period for which the audit log is retained, including the extent of logged information, depends on the system settings.

Nature of the processing

Processing activities including hosting, storage, transmission, transformation, structuring, deletion, pseudonymizatin, anonymization, making available for use, accessing for troubleshooting and others as required and in such a way that allows the controller, and end users use the YSoft Clerbo in accordance with the contractual terms governing the offering of YSoft Clerbo to the controller. Details of the technical implementation of the processing activities are described in the respective Technical Documentation (service specification data sheets) disclosed to the controller.

Purpose(s) for which the personal data is processed on behalf of the controller

Provision of YSoft Clerbo application in SaaS mode, hosting, and support services under the contractual terms governing the offering of YSoft Clerbo application to the controller.

Duration of the processing

Duration of the processing (retention period) is under control of the controller. Unless instructed otherwise, processor will process the personal data for the duration of the purpose under which the particular processing activity is performed and 30 calendar days thereafter.

Following the lapse of the retention period, processor will delete and irreversibly erase all personal data. This requirement shall not apply for personal data that are stored for the duration of processor’s backup policies and to the extent processor must retain data for evidentiary purposes in relation to the tax authorities and in connection with accounting transactions and other purposes required under applicable laws.

Processor may provide tools to allow the controller and/or its customers to export their data including Personal Data. In the event controller or controller’s customer opts not to use such tools and instead requests processor returns the personal data, processor will provide assistance to return such data, at the requesting subject expense.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Purpose	Protocol
Client interaction with Clerbo	HTTPS

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- The employees of the sub-processor have the obligation to comply with the data secrecy
- Choice of the sub-processor under the consideration of diligence especially regarding data security
- Ongoing monitoring of the sub-processors and their work
- Vulnerability and patch management is performed on weekly basis
- Regular penetration testing is conducted by 3rd party
- Existence of vulnerability and patch management standard
- Existence of Capacity Management standard

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (applicable for the deployment scenario where processor manages hosting services, for the other deployment scenarios the below listed measures will be applied proportionally)

- Generating backup copies in regular intervals
- Policy that ensures the generation and verification of backup copies with regard to availability, recoverability and data integrity (data recovery procedures)
- Checking to restorability of backup copies in regular intervals
- Storage of backup copies outside the hosting environment in a safe location
- Central procurement of hardware and software (IT architecture is planned exclusively by the IT department)
- Updating the software used to the latest version (e.g. through updates, corrections, bug fixes, etc.)
- Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and approval are in force
- Set up of the server in a separately secured server room or data centre
- Formal releasing procedures for hardware, software and IT procedures
- Existence of an emergency plan (backup contingency plan, testing of data recovery)

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Separation of productive and test system
- Rights and role concept for database access considering the principle of restriction to necessary accesses
- Logically separated storage of the data of different controllers (client separation)
- Existence of Security Testing standard
- Ongoing monitoring of the sub-processors and their work
- The employees of the sub-processor have the obligation to comply with the data secrecy
- Choice of the sub-processor under the consideration of diligence especially regarding data security

Measures for user identification and authorisation

- Establishing access authorizations for employees and third parties, including the respective documentation
- Granting of user-specific access needs authorization by asset owners
- A user/applicant/human has a unique, identifiable account.
- Two factor identification
- Individual, personalized logins for applications
- Solely authorized and privileged employees have access to the data processing systems

Measures for the protection of data during transmission

- Implementation of filter measures (URL filter, filtering of e-mail attachments)
- Diligent selection of courier services, personal pickup and accomplishing of the transport
- Encryption of data carriers / separate transfer of decryption key
- Prohibition to carry bags, etc. into the restricted area and effective enforcement of the prohibition
- Transmission of data in encrypted form using TLS 1.3
- Documentation of the remote locations / destinations to which a transmission is intended and the transmissions path (logical path)

Measures for the protection of data during storage

- Policy regarding usernames and strong passwords, which includes the topics password length and password change.
- Process for checking and approving the use of new software
- Encryption of data and data carriers
- Encryption

Purpose	Protocol
Client interaction with Clerbo	HTTPS

Measures for ensuring physical security of locations at which personal data are processed

- Diligent selection of security staff, cleaning staff and gatekeepers
- Electronic access monitoring (e.g. light barriers, motion detectors)
- Access and escort regulations for third parties (technicians, visitors, customers, cleaning staff, workmen, etc.)
- Providing that all entrances to the data processing facilities (rooms, houses, computer hardware and associated facilities) are capable of being locked
- Physical security measures to restrict entrance and access to the areas where data carriers are located
- Identity check by authorized employees (e.g. also reception desk, security service)
- Security alarm system or other appropriate security measures even after the working time
- Securing the decentralized data processing equipment (e.g. personal computers, laptops, etc.)
- Protection and restriction of access path by an access control system
- Constructional measures (fencing, surveillance cameras, locked doors, building shafts, gates and windows, etc.)
- Alarm in case of unauthorized access to server rooms

Measures for ensuring events logging

- Electronic logging and recording of data processing, in particular the input, modification and deletion of data (audit trails).
- Electronic logging and recording of the use of administration and management tools
- A register is held in which all applications that can be used for data manipulation (input, modification and deletion) are recorded.
- Allocation of authorizations for the input, modification and deletion of data based on an authorization concept
- Existence of a Logging and Monitoring standard

Measures for ensuring system configuration, including default configuration

- Protection of internal networks against unauthorised access by firewall
- Logging and documentation of accesses
- Management of access rights by a number of administrators restricted to the minimum
- Protective measures for the data input as well as for the reading, blocking and deletion of stored data
- Using VPN-technology
- Policy for the creation of strong passwords, either distributed to all employees or technically enforced
- Separation of production and test environment for databases and files
- Use of intrusion detection systems, anti-virus-systems, hardware- and software-firewall and central smartphone administration software (e.g. to delete data by remote access)

Measures for internal IT and IT security governance and management

- Established Information Security Steering committee
- Appointment of a security officer

- Establishing access authorizations for employees and third parties, including the respective documentation
- Separation of tasks / functions between the IT department and other departments
- Clear distinction between the controller´s and the processor´s areas of responsibility
- Existence of an emergency plan (backup contingency plan)
- Regular training of employees in data protection matters
- Policy on reporting a breach of the protection of personal data pursuant to Art. 33 GDPR
- Written undertaking by employees to observe data confidentiality or employees under an appropriate statutory obligation of confidentiality according to Article 28 (3) point b GDPR
- Appointment of a data protection officer

Measures for certification/assurance of processes and products

- ISO27001 Certification
- SD PAC Certification governing the secure software development lifecycle

Measures for ensuring data minimisation

- Existence of a Data privacy policy and data security concept

Measures for ensuring data quality

- Electronic logging and recording of data processing, in particular the input, modification and deletion of data (audit trails).
- Electronic logging and recording of the use of administration and management tools
- A register is held in which all applications that can be used for data manipulation (input, modification and deletion) are recorded.
- Allocation of authorizations for the input, modification and deletion of data based on an authorization concept.

Measures for ensuring limited data retention

- Implemented in compliance with GDPR
- Existence of a Data retention standard

Measures for ensuring accountability

- Existence of defined ISMS Roles and Responsibility

Measures for allowing data portability and ensuring erasure

- Existence of Database security standard
- Irreversible deletion of data carriers before reuse
- Secure erasure or destruction of all deletable data and electronic media (e.g. notebooks and laptops, hard disks, CDs, DVDs, USB sticks, audio tapes, data carriers, memory cards, etc.) after the contractually agreed end of the services

Up-to-date list of Sub-processors available at https://www.ysoft-clerbo.com/privacy-statement

Sub-processor		Description of processing activities	Sub-processor location
The respective Microsoft entity: **Microsoft Ireland Operations, Ltd.** Attn: Data Protection One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland		Regionalized cloud hosting, analytics.	Microsoft West Europe Region Reference: https://azure.microsoft.com/en-us/global-infrastructure/geographies/#geographies Hosting of EU GDPR protected personal data will only be with Microsoft Ireland unless actively changes by the end-customer.