**VERSION: 11.0 AUGUST 2026**

# DATA PROCESSING ADDENDUM

between

**Customer** as defined in the applicable Order (hereinafter "**Controller**")

and

**BRYTER US Inc.**, 33 Irving Place, Suite 5007, New York, NY 10003, (hereinafter „**Processor**")

(together also referred to as the "**Parties**" and each also referred to as a "**Party**")

In consideration of the mutual obligations set out herein and in the MSA, the parties hereby agree that, as more fully set forth below, this Addendum is added to the MSA and, where applicable, sets forth the terms and conditions under which Processor may receive and process Personal Data from Controller. References to the MSA in this Addendum shall, unless the context requires otherwise, be construed as referring to the MSA as amended and supplemented by this Addendum.

## 1. Definitions

1.1. The capitalized terms used in this data processing addendum ("**DPA**") shall have the meaning as set forth in the definitions set out in the Definitions (Appendix 1) and in the Master Service Agreement.

1.2. "**Data Protection Laws**" means all applicable laws and regulation regarding data protection, privacy or security, including those regarding the Processing of Personal Data, as amended, supplemented, replaced or superseded from time to time, including but not limited to the EU General Data Protection Regulation ("**GDPR**"), the UK General Data Protection Regulation, the UK Data Protection Act of 2018, the California Consumer Privacy Act, and laws and regulations implementing, amending or supplementing each of the foregoing, to the extent in connection with the provision of Services under the MSA, unless otherwise implied (e.g. by context of a reference or as explicitly stated).

1.3. "**Controller**", as attributed to Customer, has the general meaning of a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

1.4. "**Processor**", as attributed to BRYTER, hast the general meaning of a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

## 2. General provisions

2.1. Processor processes Personal Data on behalf of Controller for the delivery of the BRYTER Software and/or Professional Services within the meaning of the Master Service Agreement, the Definitions (Appendix 1) and the applicable Order and/or SOW (jointly referred to as the "**MSA**") according to the Data Protection Laws solely based on this DPA.

2.2. The subject-matter of the processing is set out in the MSA.

2.3. Provisions of the GDPR shall apply to and be part of this DPA if and to the extent as explicitly referenced herein, e.g. to concretize obligations under this DPA. For the avoidance of doubt, this shall not influence the potential general applicability of the GDPR as part of the Data Protection Laws.

2.4. The duration of the Processing shall be in accordance with Controller's instructions and the terms of the MSA including the DPA.

## 3. Nature and purpose of the Processing, type of Personal Data and categories of data subjects

3.1. The scope and duration and the detailed stipulations on the type and purpose of Processing shall be governed by the MSA including the DPA. Specifically, Processing shall include the following Personal Data:

| Type of Personal Data | Categories of data subjects affected | Purpose of Processing | Duration of Processing |
|---|---|---|---|
| Contact/account data (e.g. first name, last name, business email, user ID, role, tenant ID) | Authorized Users; End Users, if a login is required | Functionality and security; Access control | Until termination of MSA |
| Authentication and access credentials (e.g. password hash, login credentials) | Authorized Users; End Users, if a login is required | Functionality and security; Access control | Until termination of MSA |
| Network/device identifiers and security data (e.g. IP address, sessions IDs, timestamps, device/browser identifiers, performance metrics, log files and audit trails) | Authorized Users; End Users, if a login is required | Functionality and security; Service monitoring; Error analysis; Audit logging compliance | For security/audit logs up to 90 days where applicable, otherwise until termination of MSA |

| Type of Personal Data | Categories of data subjects affected | Purpose of Processing | Duration of Processing |
|---|---|---|---|
| Customer-provided content and derived content (e.g. uploaded documents, free text, case records, forms/workflows, extracted fields/structured content, AI output to the extent containing personal data) | Authorized Users; End Users, if a login is required; Data subjects identifiable with Customer Content (e.g. Customer employees who are not End Users, business partners of Customers) | Provision of the Software and AI Services on Controller's documented instructions; Storage, display, transformation and transmission as required by the Software's functionality; Quality assurance, error analysis and monitoring of AI-powered processing (LLM observability), to the extent necessary to ensure the functionality, stability and security of the Software | Until termination of MSA and deletion in accordance with Section 12 DPA |

3.2. Additionally, Processor's Software may be used by Controller to process any Personal Data determined by the Controller or voluntarily provided by the End User and/or Authorized User. Processor has no influence on the scope of such additional Personal Data being processed. The type of Personal Data that will be processed with Processor's Software in addition to the data set out in 3.1. above is the sole responsibility of the Controller with regard to determining its lawfulness and purpose under the GDPR. This shall not limit the Processor's obligations to implement appropriate technical and organizational measures and to process all Personal Data solely on documented instructions of the Controller in accordance with the GDPR.

3.3. Processor is prohibited from processing Personal Data for any purpose other than for the specific purpose of performing the services specified in the MSA, as amended and

supplemented from time to time, or as otherwise permitted by this DPA or Data Protection Laws.

## 4. Scope and Responsibility

Processor shall process Personal Data on behalf of Controller. Such Processing shall include actions as may be specified in the MSA. Within the scope of the MSA, Controller shall be solely responsible for complying with the statutory requirements relating to the lawfulness of Processing, in particular regarding the transfer of Personal Data to the Processor (acting as Controller).

## 5. Controller's rights and obligations

5.1. It is within the sole responsibility of Controller to assess the lawfulness of the Processing. This includes ensuring that any Processing of special categories of personal data pursuant to Article 9 GDPR is lawful and based on an applicable derogation under Article 9(2), and that appropriate safeguards are implemented. If not set out differently in the MSA, this includes the handling of data subjects' rights requests. Processor shall forward immediately to Controller any such request discernibly addressed to Controller.

5.2. Controller agrees that the MSA including the DPA, along with Controller's use of the Software, are Controller's complete documented instructions to Processor for the processing of Personal Data. Controller may issue additional instructions if required by Data Protection Laws.

5.3. Any instructions given by Controller shall be in writing or in a documented electronic form. Oral instructions shall be confirmed immediately in writing or in a documented electronic form. Changes of the subject-matter of the Processing or of procedures shall be coordinated between Controller and Processor and established in writing or in a documented electronic form.

5.4. Processor ensures that Controller, or a qualified third party instructed by Controller which is obliged to maintain confidentiality, can verify the compliance with the Processor's obligations laid out in the Data Protection Laws and this DPA and the implementation and adequacy of the technical and organizational measures by Processor before and during the Processing by making available all necessary information and contribute to audits (including onsite inspections).

5.5. Audits and inspections shall, as far as possible, not hinder Processor in its normal business operations and shall not place an undue burden on Processor. In particular, inspections at Processor's premises shall not take place more than once per calendar year and only during the Processor's normal business hours without a valid reason. The Parties shall agree on inspection dates at Processor's premises. Appointments shall be made promptly upon Controller's request and during usual business and operating hours, taking into account Processor's business interests. Processor shall be entitled to reject auditors that are competitors of BRYTER, are not sufficiently qualified to conduct such an audit or are not independent. Controller acknowledges that most of the processing is done via cloud computing on the premises of Amazon AWS and Microsoft Azure (see Schedule 1). Hence, any inspection directly of or at the premises of Processor is of limited use. Upon request by Controller, Processor will initiate inspections of Amazon AWS, Microsoft Azure or other Sub-processors in accordance with the respective DPAs concluded with those Sub-processors and as required by the Data Protection Laws.

5.6. Controller shall immediately inform Processor if errors or irregularities are detected throughout the examination.

5.7. Controller shall pay for any of Processor's costs reasonably incurred by an onsite inspection according to 5.4 or 5.5.

5.8. Controller shall notify Processor in sufficient detail and without undue delay of any defect or irregularity detected by Controller in Processor's provision of the Software concerning data protection.

BRYTER

## 6. Processor's obligations

6.1. Processor processes Personal Data solely within the scope of this DPA and on documented instructions of Controller, unless otherwise required by Data Processing Law which Processor is subject to. In such a case, Processor shall inform Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

6.2. Taking into account the nature of the Processing, Processor shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, when it comes to fulfilling the rights of data subjects in accordance with the Data Protection Laws by Controller.

6.3. Taking into account the nature of processing and the information available to Processor, Processor shall assist Controller with its obligations concerning the security of processing under the Data Protection Laws as well as its obligation to carry out a data protection impact assessment and prior consultation, where necessary. Processor shall immediately forward the required information to Controller.

6.4. Processor shall ensure that each person authorized to process Controller's Personal Data is bound to adequate contractual or statutory confidentiality obligations, informs them of all relevant data protection obligations according to this DPA and takes steps to ensure that they process them only on Controller's instructions, except where they are required to process it under the Data Protection Laws.

## 7. Processor's notification obligations

7.1. Processor shall immediately inform Controller if, in its opinion, an instruction infringes Data Protection Laws. Processor is entitled to suspend the execution of such an instruction until Controller confirms it in writing. If Controller insists on the execution of an Instruction in spite of the reservations expressed by Processor, Controller shall indemnify Processor against all damages and costs incurred by Processor in executing Controller's instruction.

The defense and claim handling shall be coordinated in good faith between the Parties and subject to the dispute resolution and limitation of liability provisions in the MSA.

7.2 Processor shall notify Controller without undue delay, and, where feasible, within seventy-two (72) hours after becoming aware of a Personal Data breach affecting Personal Data, providing Controller with sufficient information to allow Controller to meet any obligations to report to a competent authority and/or inform data subjects of the Personal Data breach under the Data Protection Laws. Such notification shall as a minimum:

(a) describe the nature of the Personal Data breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

(b) communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;

(c) describe the likely consequences of the Personal Data breach; and

(d) describe the measures taken or proposed to be taken to address the Personal Data breach.

Processor shall make reasonable efforts to obtain the relevant information from Sub-processors in a timely manner but shall not be liable for delays caused by third parties.

7.3 Processor shall co-operate with Controller and take such reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data breach.

7.4. Taking into account the nature of processing and the information available to Processor, Processor shall assist Controller regarding Controller's obligations to report personal data breaches to the competent authorities and to notify the person affected by a personal data breach in accordance with the Data Protection Laws, if they provide for such obligations.

7.5. Controller shall pay for any non-insignificant costs incurred by making use of Processor's obligation to support Controller according to section 7.4. as far as the obligation does not arise due to a violation of Data Protection Laws or this DPA by Processor.

**8. Processor's obligation to maintain professional secrecy**

8.1. This Section 8 shall only apply if, under applicable law, the Controller is subject to professional secrecy obligations arising from its professional status (such as legal, tax, healthcare, or other confidentiality obligations under national law).

8.2. Under the MSA including the DPA, Processor may process Professional Secrets. Controller shall be responsible to assess whether any data provided to Processor is deemed a Professional Secret and to notify Processor accordingly. However, Processor shall treat all data as potentially subject to professional secrecy obligations unless clearly determined otherwise.

8.3. Processor undertakes to only access or otherwise become capable of obtain knowledge of Professional Secrets to the extent strictly necessary for the performance of the obligations set out in the MSA including the DPA. For the purposes of this clause, 'obtaining knowledge' shall also include any technical or organizational access to Professional Secrets, regardless of whether actual human review occurs.

8.4. Processor undertakes to maintain confidentiality about Professional Secrets, to keep Professional Secrets strictly confidential and to take adequate measures to protect Professional Secrets from unauthorized access by third parties.

8.5. Processor may disclose Professional Secrets to Sub-processors to the extent necessary for the performance of the obligations set out in the MSA including the DPA, provided that (i) each Sub-processor has been contractually prohibited in writing (digitally sufficient) from disclosing Professional Secrets to unauthorized third parties and (ii) Sub-processor must obligate their Sub-processors accordingly.

8.6. Processor shall ensure that all employees and other persons working for Processor who are involved in the processing of Professional Secrets, have undertaken in writing (digitally sufficient) not to disclose any Professional Secrets of which they have become aware in the course of or on the occasion of their work to unauthorized third parties.

**9. Sub-processors**

9.1. Controller hereby generally authorizes Processor's use of Sub-processors. By signing this DPA, Controller authorizes Processor's use of Sub-processors listed in Schedule 1. Depending on the services outlined in the MSA, Processor will use different Sub-processors.

9.2. Controller hereby generally authorizes Processor's use of Sub-processors. Processor shall, prior to the use of any additional Sub-processor or the replacement of an existing Sub-processor, inform Controller of the intended change by written notice via e-mail during the term of the MSA. Such notice shall be sent to the e-mail address designated by Controller for DPA-related notifications.

9.3. Controller shall be entitled to object to any change in the usage of Sub-processors notified by Processor within 20 business days for materially important reasons solely. Where Controller does not object to such change within such period of time, Controller shall be deemed to have authorized such change. Where a materially important reason for Controller's objection exists, and failing an amicable resolution of this matter by the Parties, Processor shall be entitled to, at its choice, provide the services under the MSA without the use of the respective Sub-processor or to terminate the MSA at the time of the planned use of the respective Sub-processor.

9.4. Processor shall contractually ensure that Processor's obligations agreed on in this DPA also apply to all approved Sub-processors.

9.5. Processor shall remain liable to Controller for its Sub-processors' obligations.

9.6. With the execution of this DPA, Controller agrees to the use of Amazon Web Services (AWS) EMEA SARL ("AWS") and Microsoft Azure as Sub-processors. In the relationship between Processor and AWS, the AWS GDPR Data Processing Addendum applies. In the relationship between Processor and Microsoft Azure, the Microsoft Products and Services Data Protection Addendum applies. Both the AWS GDPR Data Processing Addendum and the Microsoft Products and Services Data Protection Addendum will be submitted to Controller by Processor upon Controller's explicit request.

9.7. Controller acknowledges that the use of AWS (or a substitute Sub-processor) and Microsoft Azure (or a substitute Sub-processor) is crucial to the performance of the service carried out by Processor. In case that Controller withdraws its agreement regarding the use of AWS (or a substitute Sub-processor) and/or Microsoft Azure (or a substitute Sub-processor) as Sub-processors, the Processor shall be entitled to terminate extraordinarily the MSA and this DPA as well as any other potential agreement between the Parties immediately. In case of such termination, Processor is entitled to demand the full fees payable by the Controller under the MSA or any other agreement that is terminated for the full term agreed upon between the Parties.

**10. Transfer of Personal Data to third countries.**

Personal Data shall be generally processed in the area indicated by the Hosting Services as agreed on in the specific MSA.

**11. Technical and organizational measures in accordance with obligations to ensure the security of processing**

11.1. Taking into account the state of the art, the costs of implementation and – as far as known to Processor – the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, Processor shall implement appropriate technical and organizational measures to ensure a level of security for the Personal Data appropriate to the risk.

11.2. Prior to the beginning of the Processing, Processor shall implement the technical and organizational measures listed in Art. 32 GDPR and maintain them for the duration of the MSA.

11.3. Since the technical and organizational measures are subject to technical progress, Processor is entitled and obligated to implement alternative, adequate measures in order not to fall below the security level of the measures specified in Schedule 2. If Processor makes significant changes to the measures specified in Schedule 2, he will inform Controller of such changes in advance.

11.4. Controller is responsible to verify the technical and organizational measures taken by Processor, in particular whether these are also sufficient with regard to circumstances of Processing.

**12. Obligations of Processor after termination of the MSA.**

12.1. After termination of the MSA, Processor shall, at Controller's choice and in accordance with the Data Protection Laws, delete or return and delete existing copies of all Personal Data, documents and Processing or usage results in connection with the Processing being in its possession, unless the Data Protection Laws require storage of the Personal Data.

12.2. However, Processor shall be entitled to keep backup copies of such Personal Data or information for a period of 30 days, provided that the storage of such backup copies is technically feasible with regard to Art. 32 GDPR. Notwithstanding Section 2.4., the rights and obligations of the Parties under this DPA with regard to the backup copies shall continue to apply for this period.

**13. Liability.**

Any provisions on the Parties' liability set out in the MSA shall also apply to the Processing under this DPA, unless expressly agreed upon otherwise.

**14. Final provisions.**

14.1. Where the Personal Data become subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Processor's control, Processor shall notify Controller of such action without undue delay. Processor shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Controller's sole property and area of responsibility, that data is at Controller's sole disposition, and that Controller is the responsible body in the sense of the Data Protection Laws.

14.2. Section 16 (General Provisions) of the MSA shall apply accordingly to this DPA.

14.3. If this DPA contradicts other agreements concluded between the Parties, the provisions of this DPA shall take precedence. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

[signature page immediately follows]

BRYTER

BRYTER

Signature

Name

Position Title

Date

Controller

Signature

Name

Position Title

Date

BRYTER

**Schedule 1**

**-**

**List of Sub-processors**

| **Sub-processor** | **Service Provided** | **Corporate Location** | **Sever Location** |
|---|---|---|---|
| Amazon Web Services (AWS) EMEA SARL | Cloud Server | 8 Avenue John F. Kennedy, L-1855 Luxembourg | Frankfurt am Main (Germany) |
| UAB ConvertAPI | File Converting Processor | Lauksargio g. 111, LT-10105 Vilnius, Lithuania | Frankfurt am Main |
| DeepL SE | Translation tool (add on) | Maarweg 165, 50825 Köln, Germany | Germany and Sweden |
| DataDog Inc. | Monitoring Tool | 620 8th Avenue, 45th Floor, New York, NY 10019-1741, USA | Frankfurt am Main (Germany) |
| Microsoft Azure | Cloud Server for BEAMON | Takeda Ireland Ltd (Grange Castle), New Nangor Road, Grange, Dublin 22, Ireland | Central-Gavle (Sweden) Schiphol (Netherlands) |
| Tavily | Web Search Processor for BEAMON | 33 W 60th St, New York, NY 10023, USA | USA |

BRYTER

Schedule 2

Technical und organizational measures

**Usage of AWS and Microsoft Azure**

For data security measures concerning the servers where the BRYTER Software is located please refer to technical and organizational measures of AWS and / or Microsoft Azure.

**Amazon Web Services EMEA Sarl, 8 Avenue John F. Kennedy, L-1855 Luxembourg**

**Microsoft Azure, Takeda Ireland Ltd (Grange Castle), New Nangor Road, Grange, Dublin 22, Ireland**

All personal data is stored and processed in U.S. data centers of our sub-processor Amazon Web Services (AWS) and / or Microsoft Azure.

BRYTER has executed a Data Processing Addendum with AWS, namely "AWS GDPR DATA PROCESSING ADDENDUM". BRYTER has executed a Data Processing Addendum with Microsoft Azure, namely "Microsoft Products and Services Data Protection Addendum". Both agreements are integral parts of these technical and organizational measures. AWS is ISO 27001, 27017 and 27018 certified. Microsoft Azure is ISO 27001, ISO 27002, and ISO 27018 certified.

ISO 27018 is a code of conduct for the protection of personal data in the cloud. It is based on the ISO 27002 information security standard (the “Standard”) and serves as a guideline for the implementation of ISO 27002-controls that apply to personal data that uniquely identifies a person in the public cloud. The Standard provides additional controls and guidelines for the protection requirements of personal data that is not taken into account by the current controls of ISO 27002. By complying with this Standard, both AWS and Microsoft Azure have a system of control mechanisms that are specifically concerned with the protection of private data. By complying with this internationally recognized guide and independently reviewing it, both AWS and Microsoft Azure demonstrate their commitment to customer content privacy. Further information on our sub-processors and their certifications can be found here: https://aws.amazon.com/compliance/gdpr-center/ and https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

**1. Physical access control**

Processor is not using on-premises servers but cloud computing, currently AWS and Microsoft Azure, to provide and execute the Software and to process data entered into the Software. Thereto the following is stated to ensure physical access control:

- For data security measures concerning the physical location of the servers where the BRYTER Software is located please refer to the AWS and/or Microsoft Azure technical and organizational measures as stated above.
- Electronic data storages are safely deleted after their usage.

- The entrance of the office building by the public is prevented through doors that have opening systems through a key or an equivalent device with such areas being kept closed when access to the documents included in the filing is not required.

**2. User access control to data processing systems**

To prevent unauthorized parties from using data processing systems.

- Workstation computers are secured as follows:
  - User login only through centrally controlled identity management system.
  - Workstation computers are automatically locked after a certain idle time.
  - Personal access code required to unlock computers.
- Password policy:
  - For administrative access (minimum requirements for password length and complexity, two-factor authentication).
  - For employee access (minimum requirements for password length and complexity, two-factor authentication).
  - For customer access (minimum requirements for password length and complexity).

**3. Access control to personal data in data processing systems.**

To ensure that those authorized to use a data processing system can only access the data for which they are authorized and that data, especially personal data, is not subject to unauthorized viewing, copying, modification, or deletion when it is processed or used or after it is stored.

- Central rights management, separated for system access and application access.
- Controls to prevent users from changing their own rights.
- Controls to prevent users from requesting a change without the approval of the person in charge in accordance with the established approval process.
- External access restricted to VPN- or SSH-secured connections.
- Data encrypted for storage.

**4. Separation control**

To ensure that data collected for different purposes can be processed separately.

- Separation of:
  - Employee data.
  - Customer contact data.
  - Customer test data (project work, customer developments).
  - Customer data in the BRYTER data center.
- System level:
  Customer data in data center is administered in strict separation and in separate systems (databases, etc.) from BRYTER data (including the CRM system).

- Different applications:
  Customer data and employee data is processed using separate applications.

**5. Measures for pseudonymization and encryption**

To ensure that traceability of data to individuals is at least restricted.

- Privacy-by-design and privacy-by-default measures, including the appropriate training for product teams and based on the principles of avoiding and limiting data.
- All download/upload internet connections secured through either SSL/TLS, SSH.
- Input control.

To ensure that it is possible to subsequently check and determine whether and by whom data, especially personal data, was entered into data processing systems, modified, or deleted.

- Comprehensive logging by all systems that process personal data, making it possible to subsequently determine whether and by whom personal data was entered, modified, or removed.
- Personalized user accounts extending to the specialized applications.
- Separate system logs and application logs, ruling out manipulation of the application logs at the system level.

**6. Order control**

To ensure that personal data from orders can only be processed according to the client's instructions.

- Regulation of instructions in principal service and data processing agreement.
- Administration of users and rights by client at application level.
- Transfer/entry of data by client, who decides which data is transferred and when.
- Access to this data limited to roles with corresponding access rights.
- Automated processing of data by certified software ensuring that data is processed in accordance with contracted procedure.
- Use of standardized contracts as stipulated by law for relations with customers and service providers.
- Inclusion of sub-processor with corresponding confidentiality, data processing, system access agreements.

**7. Transmission control**

To ensure that data, especially personal data, cannot be viewed, copied, modified, or deleted without authorization while it is transmitted electronically, transported, or saved to storage media and that it is possible to check and determine the intended destinations of data, especially personal data, transferred using data transmission equipment.

- All download/upload internet connections secured through either SSL/TLS, SSH.
- No local storage of personal data; all data stored centrally in the systems of BRYTER.

- External connections possible only through approved applications.
- External connections possible only through approved services.
- All remote data transfer connections logged wherever technically possible.
- Regulations for the disposal of waste with confidential content.

**8. Availability**

To ensure that data, especially personal data, is protected against random destruction or loss.

- Data encrypted for storage.
- All access authorizations and access rights of a person leaving the company are promptly blocked and if necessary deleted.
- All company-owned items relating to personal data are reclaimed from an individual leaving the company.
- Written data carriers are stored before and after dispatch in such a way that access is only possible for authorized persons.
- Regular testing of data security / backup systems, etc.
- Monitoring of AI-powered processing operations, including event-driven analysis of processing activities for error analysis, quality assurance and ensuring the performance of the language models deployed (LLM observability).

**9. Resilience**

To ensure that data processing systems are sufficiently resilient and robust.

- Inventory of processing activities with integrated assessment of consequences for data protection and assessment of the appropriateness of technical and organizational measures.
- Integration of privacy by design in product management:
  Advanced controls can be triggered by procedural manager together with the data protection officer for assessment of consequences for data protection (administration of processes including checks, coordination, analysis, and evaluation).
- Use of next-generation firewall.
- Monitoring to ensure early detection and at least limit or even prevent damage due to malware.
- For server related resilience measures please refer to the to the AWSand/or Microsoft Azure technical and organizational measures.
- Incident Response Management.

**10. Security Management**

To ensure security during processing

- Internal and external ISO 27001 audits.
- Regular checks of technical and organizational measures with responsible roles, including whether they reflect the state of the art.

- Management evaluations as a regular routine.

**11. Measures to prevent concatenation**

To ensure that data is used only for the purpose for which it was collected (purpose limitation principle)

- Use of role concept to limit processing, use, and transmission rights.
- Programmed omission or closure of interfaces in procedures and procedure components.
- Rules prohibiting backdoors, quality assurance audits to check compliance in software development.
- Functional separations based on role concept.
- Separations through role concepts with phased access rights based on identity management and a secure authentication process.
- Regular awareness training.

**12. Personal Data Protection Management**

To ensure that obligations to provide information are met

- Data Protection Management System in place with reporting lines to senior management.
- Records of processing activities in accordance with Art. 30 GDPR (both as controller and as processor).
- Data privacy statement on BRYTER website.
- Detailed information outlined in data privacy portal of BRYTER.
- Documentation of contracts with internal employees, contracts with external service providers and third parties from whom data is collected or to whom data is transmitted.