VERSION: GER 12.0 NOVEMBER 2026

DATA PROCESSING ADDENDUM

between

the customer named in the applicable Order (hereinafter "**Customer**" or "**Controller**")

and

BRYTER GmbH, Biebergasse 2, 60313 Frankfurt am Main, Germany (hereinafter "**BRYTER**" or "**Processor**")

(Customer and BRYTER together the "**Parties**", each a "**Party**").

The Controller and BRYTER have entered into an agreement on the use of the BRYTER Software and any further services (the "**MSA**").

In the course of performing the MSA, the Controller may transfer personal data to BRYTER for processing on behalf of the Controller.

This Data Processing Addendum ("**DPA**") governs the rights and obligations of the Parties with regard to the processing of such personal data pursuant to Art. 28 GDPR.

IMPORTANT NOTICE: This DPA applies to all personal data processed by BRYTER on behalf of the Controller. Where the Controller is subject to professional or official secrecy obligations, in particular under Sections 43a and 43e of the German Federal Lawyers' Act (BRAO), Sections 18 and 26a of the German Federal Notaries' Act (BNotO) and Section 203 of the German Criminal Code (StGB), Section 6 applies in addition. Section 6 prevails over the other provisions of this DPA to the extent they deviate from one another.

1. General Provisions

1.1 Customer is the controller within the meaning of Art. 4 No. 7 GDPR. BRYTER is the processor within the meaning of Art. 4 No. 8 GDPR.

1.2 BRYTER processes personal data exclusively to perform the MSA, including the applicable Orders and any project or service descriptions (Statements of Work), and on documented instructions of the Controller pursuant to Section 3.4 and Art. 28(3)(a) GDPR.

1.3 The subject matter and purpose of the processing are set out in the MSA and the agreements referred to in Section 1.2.

1.4 The duration and scope of the processing are governed by the MSA, including the applicable Orders, and the instructions of the Controller, unless otherwise provided in this DPA.

1.5 Where this DPA uses terms defined in the GDPR, the statutory definitions apply.

2. Type of Personal Data and Categories of Data Subjects

2.1 The personal data processed within the BRYTER Software result from the content and information that the Controller enters into the BRYTER Software or transmits to BRYTER. BRYTER has no influence on the type, scope or categories of personal data that the Controller provides for processing. Accordingly, all types of personal data may be processed, including special categories of personal data, provided that their processing by the Controller is permissible.

2.2 The personal data typically processed in the course of using the BRYTER Software and the groups of data subjects concerned are set out in the following overview:

Type of personal data	Categories of data subjects	Purpose of processing	Duration of processing
Contact/customer account data (e.g. first name, last name, email address, user ID, role/rights, tenant ID)	• Authorized Users • End Users, where login is required	• Functionality and security • User management • Access control	Until termination of the MSA
Authentication and access identifiers (e.g. password hash, login credentials)	• Authorized Users • End Users, where login is required	• Functionality and security • Access control	Until termination of the MSA
Network/device identifiers and security data (e.g. IP address, session IDs, timestamps, device/browser identifiers, performance metrics, log files and audit trails)	• Authorized Users • End Users, where 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 the MSA

Type of personal data	Categories of data subjects	Purpose of processing	Duration of processing
Content provided by Customer and derived content (e.g. uploaded documents/files, free text, forms/workflows, extracted fields, AI input/output, to the extent containing personal data)	• Authorized Users • End Users • Other data subjects identifiable in Customer content (e.g. Customer employees who are not End Users, business partners)	• Provision of the BRYTER Software and, where applicable, AI-supported functions on documented instructions of the Controller • Storage, display, transformation and transmission in accordance with the functional scope of the Software • Quality assurance, error analysis and monitoring of AI-supported processing (LLM observability), to the extent necessary to ensure the functionality, stability and security of the Software	Until termination of the MSA and deletion/return pursuant to Section 10 of this DPA

2.3 The categories of data subjects depend on the respective data transmitted by the Controller. Data subjects may include in particular Authorized Users of the Controller and other persons whose data the Controller has entered into the BRYTER Software (e.g. customers, employees, business partners or other third parties).

3. Rights and Obligations of the Controller

3.1 The Controller is solely responsible for ensuring that the processing of personal data in accordance with this DPA, the MSA and the applicable Order is lawful. This includes in particular reviewing and ensuring the permissibility of the processing under data protection law, including compliance with the requirements of Art. 6 and – where applicable – Art. 9 GDPR.

3.2 Where special categories of personal data within the meaning of Art. 9 GDPR are processed, the Controller shall ensure that an applicable legal basis pursuant to Art. 9(2) GDPR exists and that appropriate safeguards are taken.

3.3 Unless otherwise provided in the MSA, the Controller is responsible for handling requests from data subjects under Art. 12 to 22 GDPR. BRYTER shall forward without undue delay to the Controller any requests from data subjects that are recognizably addressed to the Controller.

3.4 The MSA and the applicable Order, including this DPA, and the use of the BRYTER Software in accordance with the contract constitute the documented instructions of the Controller within the meaning of Art. 28(3)(a) GDPR. The Controller is entitled to issue supplementary instructions to BRYTER to the extent these are necessary to comply with data protection requirements and do not conflict with the provisions of the MSA and this DPA.

3.5 Instructions of the Controller must be given in text form or in a documented electronic form. Changes to the subject matter or modalities of the processing resulting from instructions shall be agreed between the Parties and documented.

3.6 The Controller is entitled to verify BRYTER's compliance with its data protection obligations (Art. 28(3)(h) GDPR) in accordance with the applicable data protection laws and this DPA, or to have such compliance verified by a third party bound to confidentiality and professionally qualified. BRYTER shall provide the Controller with the information required for this purpose and support audits in accordance with this DPA.

3.7 Audits and inspections shall be carried out in such a way that they do not unreasonably disrupt BRYTER's business operations. On-site audits take place – unless there is a legitimate reason – no more than once per calendar year, during normal business hours and after prior coordination. BRYTER may reject auditors who are competitors of BRYTER, lack the necessary expertise or are not independent.

3.8 A substantial part of the processing of personal data takes place using cloud infrastructures, in particular Amazon Web Services and Microsoft Azure. On-site audits at BRYTER's premises are therefore only of limited suitability for verifying compliance with data protection requirements. At the Controller's request, BRYTER shall arrange audits of sub-processors within the framework of the respective existing data processing agreements and the applicable data protection requirements.

3.9 The Controller shall inform BRYTER without undue delay if, in the course of audits or otherwise, it identifies defects or irregularities in connection with the processing of personal data or raises data protection objections.

3.10 The Controller shall bear the reasonable and demonstrably incurred costs incurred by BRYTER in connection with audits or on-site inspections under this Section, unless these are attributable to a breach of data protection obligations by BRYTER.

4. Obligations of the Processor

4.1 BRYTER processes personal data exclusively within the framework of the MSA and this DPA and exclusively on documented instructions of the Controller, unless BRYTER is required to process otherwise by mandatory Union or Member State law. In such a case, BRYTER shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 Taking into account the nature of the processing, BRYTER shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible for BRYTER, in fulfilling its obligations to respond to requests for exercising the data subject's rights under Art. 12 to 22 GDPR.

4.3 Taking into account the nature of the processing and the information available to BRYTER, BRYTER shall assist the Controller in ensuring compliance with its obligations under Art. 32 GDPR and – where necessary – in carrying out a data protection impact assessment and any prior consultation under Art. 35 and 36 GDPR. BRYTER shall provide the Controller with the information required for this purpose without undue delay.

4.4 BRYTER shall ensure that all persons processing personal data of the Controller under its responsibility (i) are subject to an appropriate contractual or statutory obligation of confidentiality, (ii) are informed of the relevant data protection obligations under this DPA and (iii) process personal data exclusively on documented instructions of the Controller. By way of derogation, processing without instructions of the Controller is only permitted to the extent BRYTER is required to do so by mandatory Union or Member State law. In such a case, BRYTER shall inform the Controller of the relevant legal requirement before processing, unless the applicable law prohibits such information. With regard to compliance with professional secrecy obligations, the provisions in Section 6 of this DPA apply in addition.

4.5 Where the Controller uses functions within the BRYTER Software that are based on machine learning or other artificial intelligence techniques, the Controller remains responsible for the lawfulness of the inputs and for reviewing, assessing and using the results generated by these functions. In addition, the provisions contained in Section 10 (AI Terms) of the MSA apply to the use of such AI-supported functions; they are incorporated into this DPA by reference and apply accordingly.

4.6 Selection of the Language Model

4.6.1 Language models from several providers are available for the AI Services within BEAMON AI. The provider and the place of processing are set out in Schedule 1 to this DPA.

4.6.2 The language model is selected in two stages: (a) an Admin of the Controller determines for the respective Tenant which of the available language models are

enabled and may deactivate individual language models for the Tenant at any time. Deactivated language models are not available for selection by the BEAMON Users of that Tenant; (b) within the language models enabled by the Admin, the BEAMON User selects the language model to be used for each individual input. Both selection decisions constitute documented instructions within the meaning of Section 3.4.

4.6.3 In the default configuration, only the language models provided via Microsoft Azure (Microsoft Ireland Operations Ltd) for which processing, including inference, takes place exclusively within the European Union are enabled for each Tenant (Schedule 1). Further language models are used only after being enabled by an Admin; until then, no Customer Data is processed with these language models; in particular, no Customer Data is transferred to a model provider not already used under sentence 1.

4.6.4 The assessment of whether enabling and using a particular language model is compatible with the professional obligations incumbent on the Controller lies with the Controller. This applies to enabling under Section 4.6.2(a) and to each use under (b); by enabling a language model, the Controller opens its use to all BEAMON Users of the Tenant. Sections 3.1 and 6.2 apply accordingly. Before enabling, BRYTER shall provide the Controller with information on the model provider, the place of processing and the basis for any third-country transfer for the language model concerned.

4.6.5 For AI functions within BRYTER Workflows, in particular AI Agents, only language models within the meaning of Section 4.6.3 sentence 1 are used. Selecting one of these language models when configuring an AI Agent constitutes a documented instruction within the meaning of Section 3.4; enabling under Section 4.6.2(a) is not required. Section 4.6.4 applies accordingly, with the configuration of the AI Agent taking the place of enabling.

5. Notification Obligations of the Processor

5.1 BRYTER shall inform the Controller without undue delay if BRYTER is of the opinion that an instruction of the Controller infringes the GDPR or other applicable data protection provisions. BRYTER may suspend the execution of such an instruction until it is confirmed or amended by the Controller, to the extent necessary to avoid an infringement of the law.

5.2 If the Controller insists on the execution of an instruction despite a corresponding notice from BRYTER, the Controller shall indemnify BRYTER against all damages, costs and expenses incurred by BRYTER as a result of executing that instruction. BRYTER shall inform the Controller without undue delay of any third-party claims asserted and shall not acknowledge any such claims without the Controller's prior consent. The defence against such claims shall be conducted, at BRYTER's option, in coordination with the Controller or by the Controller itself.

5.3 Taking into account the nature of the processing and the information available to BRYTER, BRYTER shall assist the Controller by appropriate technical and organizational measures in fulfilling its obligations under Art. 33 and 34 GDPR.

5.4 Where the assistance under this Section requires effort beyond the contractually owed scope and this is not attributable to a breach of data protection obligations by BRYTER, the Controller shall bear the reasonable and demonstrably incurred costs incurred by BRYTER as a result.

6. Protection of Professional Secrets and Professional Secrecy Obligations

6.1 This Section applies in addition where the Controller is subject to professional or official secrecy obligations, in particular as a lawyer or member of a legal or tax advisory profession pursuant to Sections 43a and 43e BRAO or as a notary pursuant to Section 18 BNotO, as well as Section 203 StGB. This Section applies accordingly where the Controller is subject to comparable professional or official secrecy obligations under Swiss law, in particular under Art. 321 of the Swiss Criminal Code (StGB) and Art. 13 of the Swiss Federal Act on the Freedom of Movement for Lawyers (BGFA), or under Austrian law, in particular under Section 121 of the Austrian Criminal Code (öStGB), Section 9 of the Austrian Lawyers' Act (RAO) and Section 37 of the Austrian Notaries' Code (NO).

6.2 In the course of the MSA, the applicable Order and this DPA, BRYTER may obtain access to or knowledge of data that constitute professional secrets protected under the aforementioned provisions ("**Professional Secrets**"). The Controller remains responsible for assessing whether and to what extent the data it transmits constitute Professional Secrets. Notwithstanding this, BRYTER treats all data processed on behalf of the Controller as potentially protected by professional secrecy as a precaution, unless it is clearly established otherwise.

6.3 BRYTER undertakes to treat Professional Secrets as strictly confidential and to take note of them or make them technically accessible only to the extent strictly necessary for the proper performance of its contractual obligations. "**Taking note**" also includes any technical or organizational possibility of access, irrespective of whether natural persons actually inspect the content.

6.4 The Processor acknowledges that, where the Controller is subject to Section 203 StGB, any unauthorized disclosure or exploitation of Professional Secrets may constitute a criminal offence under Sections 203 and 204 StGB. BRYTER shall ensure that all persons at BRYTER involved in the processing of Professional Secrets have been effectively bound to secrecy and are informed of the obligations arising from this DPA and from the relevant professional and criminal law provisions, in particular Section 203 StGB and, where the Controller is subject to Swiss or Austrian law, Art. 320 and Art. 321 StGB (Switzerland) or Section 121 öStGB (Austria), respectively.

6.5 BRYTER is entitled to use sub-processors to perform the contractual services to the extent necessary. BRYTER shall ensure that all sub-processors and the persons involved in the processing of Professional Secrets are bound in advance in text form to maintain professional secrecy in accordance with this Section and that this obligation continues to apply to any further sub-processing relationships. BRYTER shall further ensure that the persons concerned are informed of the obligations and criminal law consequences arising from the relevant professional and criminal law provisions, in particular Section 203 StGB and, where the Controller is subject to Swiss or Austrian law, Art. 320 and Art. 321 StGB (Switzerland) or Section 121 öStGB (Austria), respectively.

6.6 The obligations under this Section continue without time limit, including after termination of the MSA and this DPA.

6.7 Where the Controller is a professional secrecy holder within the meaning of Section 53a of the German Code of Criminal Procedure (StPO), the Professional Secrets processed under this DPA may be subject to the right to refuse to testify under Section 53a StPO and to protection against seizure, in particular under Section 97(2) StPO. In the event of an official examination or measure, in particular a search or seizure, that is aimed at the disclosure or surrender of Professional Secrets or by which Professional Secrets are directly or indirectly affected (for example because they are located on the same physical systems), BRYTER shall, to the extent legally permissible, object, inform the intervening authority that the data concerned (also) constitute Professional Secrets, and inform the Controller without undue delay so that the Controller can decide on the further course of action.

6.8 To facilitate the classification under professional law for Austrian professionals (in particular lawyers and notaries), we additionally provide the following information documents: (a) the "Supplementary Guidance for Austrian Professionals" (Ergänzende Hinweise für österreichische Berufsträger) and (b) the "ÖRAK Checklist for AI Providers" (ÖRAK-Checkliste für KI-Anbieter). These documents serve information and explanatory purposes only; they do not create any independent contractual obligations and leave the rights and obligations of the Parties under this DPA unaffected.

6.9 To facilitate the classification under professional law for Swiss professionals (in particular lawyers and notaries), we additionally provide the "Supplementary Guidance for Swiss Professional Secrecy Holders" (Ergänzende Hinweise für schweizerische Berufsgeheimnisträger). This document serves information and explanatory purposes only; it does not create any independent contractual obligations and leaves the rights and obligations of the Parties under this DPA unaffected.

7. Sub-processors

7.1 BRYTER currently uses the external sub-processors listed in Schedule 1 to this DPA. The Controller hereby expressly consents to the engagement of the external sub-processors listed in Schedule 1.

7.2 BRYTER is also generally entitled to engage further sub-processors or to replace existing sub-processors. BRYTER shall inform the Controller of the intended change in advance in text form. The notification is sent to the email address designated by the Controller for notifications in connection with this DPA. The Controller may notify BRYTER of the relevant email address at any time in text form to legal@bryter.io.

7.3 The Controller may object to such changes for an important reason under data protection law within fifteen (15) working days of receipt of the notification. If no objection is raised within this period, consent to the intended change is deemed given. If the Controller objects and the Parties cannot reach a mutually agreeable solution, BRYTER is entitled, at its option, (i) to provide the affected services without using the sub-processor concerned or (ii) to terminate the MSA and this DPA with effect from the date of the planned engagement of the sub-processor.

7.4 Where BRYTER engages a sub-processor to carry out specific processing activities on behalf of the Controller, BRYTER shall ensure that the same data protection obligations as set out in this DPA are imposed on the sub-processor by way of a contract to be concluded in writing. The contract may also be concluded electronically and must in particular provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing meets the requirements of the GDPR.

7.5 Where the sub-processor fails to fulfil its data protection obligations, BRYTER remains liable to the Controller for the performance of the sub-processor's obligations.

7.6 BRYTER uses in particular Amazon Web Services (AWS) and Microsoft Azure as sub-processors for the operation of the BRYTER Software and for the processing of personal data under this DPA. These sub-processors are essential for the technical and organizational provision of the BRYTER Software and cannot readily be replaced. BRYTER has concluded a data processing agreement complying with the requirements of Art. 28(4) GDPR with each of Amazon Web Services (AWS) and Microsoft Azure. The respective agreements will be made available to the Controller upon request.

7.7 The provisions of Section 7.3 apply accordingly to the use of Amazon Web Services (AWS), Microsoft Azure and their respective successor or replacement providers, provided that, in the event of an objection by the Controller for an important reason under data protection law, BRYTER is not obliged to provide the affected services without using these sub-processors or by using an alternative infrastructure. If the Parties cannot reach a mutually agreeable solution in such a case, BRYTER is entitled to terminate the MSA and this DPA for good cause with effect from the date of the planned engagement of the respective sub-processor. In this case, BRYTER shall refund to the Controller, on a pro rata basis, any fees paid in advance for the period after the termination takes effect.

8. Transfer of Personal Data to Third Countries

Personal data and Professional Secrets are generally processed in Member States of the European Union or in other contracting states of the Agreement on the European Economic Area (EEA).

BRYTER is entitled to have personal data processed outside the European Union or the EEA, or processed by sub-processors outside the European Union or the EEA, if and to the extent the requirements of Art. 44 et seq. GDPR are met.

BRYTER shall ensure that, in the event of a transfer of personal data to third countries, appropriate safeguards within the meaning of Art. 46 GDPR are in place, for example through the conclusion of standard data protection clauses adopted by the European Commission, or that an adequacy decision pursuant to Art. 45 GDPR exists.

Where personal data are processed in third countries in the course of engaging sub-processors, BRYTER shall ensure that these sub-processors are contractually obliged to maintain a level of data protection equivalent to the GDPR.

Where a language model is enabled for a Tenant pursuant to Section 4.6 whose model provider carries out the processing outside the European Economic Area, the transfer is safeguarded by appropriate safeguards within the meaning of Art. 46 GDPR; the standard data protection clauses of the European Commission provided by the respective model provider are decisive. The place of processing is set out in Schedule 1.

9. Technical and Organizational Measures pursuant to Art. 32 GDPR

9.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, BRYTER shall implement appropriate technical and organizational measures pursuant to Art. 32 GDPR to ensure a level of security for the personal data appropriate to the risk.

9.2 The technical and organizational measures implemented by BRYTER are described in more detail in Schedule 2 to this DPA; they are implemented before the processing begins and maintained for the term of the MSA.

9.3 Technical and organizational measures are subject to technical progress and further development. BRYTER is entitled and obliged to adapt them to the state of the art during the term of the MSA, provided that the level of security described in Schedule 2 is not undercut.

9.4 BRYTER shall bring to the Controller's attention in an appropriate manner any changes to the technical and organizational measures that materially affect the agreed level of security; this may also be done electronically.

9.5 Customer is responsible for assessing the suitability of the technical and organizational measures taken by BRYTER with regard to the specific circumstances of the processing.

10. Deletion and Return of Personal Data after Termination of the MSA

10.1 After termination of the MSA, BRYTER processes personal data only if and for as long as this is necessary for the winding-up of the contractual relationship or for compliance with statutory retention obligations.

10.2 At the Controller's choice, BRYTER shall, after termination of the MSA, either delete all personal data processed on behalf of the Controller in compliance with data protection law or return it to the Controller and delete existing copies, unless there is a statutory obligation to continue storing it. Statutory retention obligations under the law of the European Union or a Member State remain unaffected.

10.3 By way of derogation from Section 10.2, BRYTER is entitled to retain backup copies of personal data for a period of up to 30 days after termination of the MSA where immediate deletion from these backup copies is not possible for technical reasons. The provisions of this DPA continue to apply without restriction during this period.

11. Liability

The liability provisions agreed between the Parties in the MSA apply accordingly to the processing of personal data under this DPA, unless mandatory data protection provisions preclude this.

12. Final Provisions

12.1 If the personal data transmitted by the Controller to BRYTER become the subject of attachment, seizure, insolvency or composition proceedings or other measures by third parties during processing, BRYTER shall inform the Controller thereof without undue delay, unless prohibited by a statutory obligation. In such a case, BRYTER shall inform the parties involved without undue delay that the power of disposal over the data concerned lies exclusively with the Controller, that these data fall within the Controller's sphere of responsibility and that the Controller is the controller within the meaning of Art. 4 No. 7 GDPR.

12.2 If and as long as professional secrecy obligations of the Controller – in particular under Sections 43a and 43e BRAO, Sections 18 and 26a BNotO and Section 203 StGB – are

affected, the provisions of this DPA apply accordingly to Professional Secrets and other confidential information within the meaning of Section 6 of this DPA.

12.3 To the extent provisions of this DPA conflict with provisions of the MSA, the provisions of this DPA prevail over the provisions of the MSA.

12.4 In all other respects, the final provisions of the MSA apply accordingly to this DPA.

12.5 Should individual provisions of this DPA be or become invalid or unenforceable in whole or in part, the validity of the remaining provisions remains unaffected. The Parties undertake to replace the invalid or unenforceable provision with a valid provision that comes closest to the commercial purpose of the invalid provision.

Schedule 1

-

List of Sub-processors

The sub-processors listed below are used by BRYTER to provide the BRYTER Software. They are used exclusively within the scope of the Controller's instructions and in accordance with the provisions of this DPA.

Sub-processor	Service provided	Company location	Server location
Amazon Web Services (AWS) EMEA SARL	Cloud infrastructure (hosting, operation and storage of the BRYTER Software)	8 Avenue John F. Kennedy, L-1855 Luxembourg	Frankfurt am Main (Germany)
Anthropic Ireland, Limited	Provision of the optional Claude language model in BEAMON; available only after being enabled by an Admin of the Controller	6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland	United States of America
DataDog Inc.	Monitoring and analysis tool (system and usage metrics)	620 8th Avenue, 45th Floor, New York, NY 10019-1741, USA	Frankfurt am Main (Germany)
DeepL SE	Translation service (optional, in accordance with the BEAMON AI Terms of Use)	Maarweg 165, 50825 Cologne, Germany	Germany and Sweden
Microsoft Azure (Microsoft Ireland Operations Ltd)	Cloud infrastructure and default LLM service in BEAMON as well as language	One Microsoft Place, South County Business	Data centre regions within the European Union

	models for AI functions of BRYTER Workflows	Park, Leopardstown, Dublin 18, Ireland	
UAB ConvertAPI	API-based conversion service	Lauksargio g. 111, LT-10105 Vilnius, Lithuania	Frankfurt am Main (Germany)
Verlag Dr. Otto Schmidt KG	API interface to Otto Schmidt publishing data (optional, in accordance with the BEAMON AI Terms of Use)	Gustav-Heinemann-Ufer 58, 50968 Cologne, Germany	Germany

Schedule 2

-

Technical and Organizational Measures

BRYTER takes appropriate technical and organizational measures within the meaning of Art. 32 GDPR to ensure a level of security appropriate to the risk for the personal data processed on behalf of the Controller.

The measures take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing and are regularly reviewed and further developed.

1. Physical Access Control

To prevent unauthorized physical access to processing facilities, BRYTER takes in particular the following measures:

- The BRYTER Software is operated exclusively in secured data centres of cloud infrastructure providers that use physical security measures such as access controls, surveillance systems and access logging.
- Physical access to the office premises used by BRYTER is restricted to authorized persons.
- Unauthorized persons are denied access to areas in which personal data may be processed.

2. System Access Control (User Access)

To prevent the use of processing systems by unauthorized persons, BRYTER implements in particular the following measures:

- use of central identity and access management to control user access;
- assignment of access rights based on a role-based authorization concept;
- use of appropriate authentication mechanisms, including additional security factors, where technically and organizationally appropriate;
- blocking or revocation of user accounts in the event of inactivity or upon termination of the employment or contractual relationship.

3. Data Access Restriction

To ensure that authorized persons can access only the personal data released to them, in particular the following measures are implemented:

- separation of system and application rights and restriction of access to personal data on a need-to-know basis;
- use of technical and organizational measures to prevent unauthorized viewing, modification or deletion of personal data;
- logging of relevant access and processing operations;
- encryption of stored personal data, where technically and organizationally appropriate.

4. Separation Control

For the separate processing of data collected for different purposes, BRYTER uses in particular the following measures:

- logical separation of tenant, project and customer data;
- separation of customer, test and internal company data;
- use of separate systems, databases or applications for different data categories, where necessary.

5. Transfer and Disclosure Control

To ensure the confidentiality of personal data during transmission, BRYTER takes in particular the following measures:

- securing data transmissions by means of appropriate encryption technologies;
- restriction of external connections to approved, controlled and documented interfaces;
- avoidance of uncontrolled local storage of personal data on end devices.

6. Input Control

To ensure traceability of whether and by whom personal data have been entered, modified or deleted, in particular the following measures are used:

- logging of relevant processing operations in the systems used;
- use of personalized user accounts for the unambiguous attribution of processing actions;
- separation of application and system logs to prevent unauthorized manipulation.

7. Availability Control

To protect personal data against accidental destruction or loss, BRYTER takes in particular the following measures:

- performance of regular data backups;
- maintenance of recovery procedures and contingency plans;
- regular review of backup and restart processes;
- prompt revocation of access rights upon termination of employment or contractual relationships.

8. Resilience of Systems

To ensure the resilience and robustness of the processing systems, BRYTER implements in particular the following measures:

- monitoring of systems for the early detection of security events;
- established procedures for handling security incidents (incident response);
- use of appropriate protection mechanisms at infrastructure and application level;
- monitoring of AI-supported processing operations, including case-by-case evaluation of processing operations for error analysis, quality assurance and ensuring the performance of the language models used (LLM observability).

9. Order Control

To ensure that personal data are processed exclusively in accordance with the Controller's instructions, in particular the following measures are taken:

- definition and documentation of rights to issue instructions in the MSA and in this DPA;
- contractual obligation of employees and sub-processors to maintain confidentiality and data protection;
- controlled and documented engagement of sub-processors.

10. Data Protection Management

To ensure compliance with data protection obligations, BRYTER implements in particular the following measures:

- operation of a data protection management system with defined responsibilities;

- maintenance of records of processing activities pursuant to Art. 30 GDPR;
- regular review and further development of the technical and organizational measures;
- training and awareness-raising of employees in the field of data protection and information security.

11. Use of Cloud Infrastructure

BRYTER uses cloud infrastructures, in particular from Amazon Web Services (AWS) and Microsoft Azure, to provide the BRYTER Software. These providers in turn use appropriate technical and organizational measures and hold recognized security certifications. BRYTER has concluded corresponding data processing agreements with these providers.