



## Legal Terms for purchase via Stripe (“Stripe Legal Terms”)

When buying BRYTER products via Stripe Technology Company Limited (STC) (“Stripe”) the following terms shall apply:

### 1. General

Unless defined in the Stripe Legal Terms, definitions are set out in [Appendix 1 \(Definitions\)](#), which are incorporated into the Stripe Legal Terms by reference.

The subscription period stated on the invoice received upon successfully buying BRYTER products via Stripe corresponds to the Initial Term as defined in the applicable Master Service Agreement (“MSA”) and the Definitions. Any subsequent renewal terms, if applicable, will be invoiced accordingly in accordance with the MSA.

The legal terms linked on this page constitute the current version of the applicable Stripe Legal Terms of use in each case. The version in force at the time the contract is concluded shall apply to the respective contractual relationship. Customers can view the version number on the page of the relevant document and also have the option to access previous versions there. In addition, the current version can be downloaded via the download button available on the page of the respective document.

Notwithstanding section 15.2 of the MSA, for Order Forms with an Initial Term of one (1) month concluded via the payment service provider Stripe, the following shall apply: the Order shall automatically renew for successive one-month periods unless terminated by either Party at any time with effect from the end of the then-current calendar month. Upon effectiveness of such termination, access to and use of the Software will cease and any fees incurred or accrued up to the effective termination date remain payable. All other provisions of the MSA shall remain unaffected.

### 2. BEAMON AI

For purchases of BEAMON AI (Assist and / or Extract) the following terms shall apply:

1. [Master Service Agreement \(Germany\)](#)
2. [Definitions](#)
3. [Support and Maintenance Services](#)
4. [Data Processing Addendum \(Germany\)](#)
5. [Privacy Policy](#)

### 3. OSV Integration



For purchases of the OSV Integration, in addition to the listed terms above, the following terms shall apply:

1. [OSV Integration Terms](#)
2. [Nutzungsbedingungen für Otto Schmidt Legal Data Hub](#)

*Last updated: April 2026*

## MASTER SERVICE AGREEMENT

This master service agreement (the “**MSA**”) sets out the entire agreement which governs the contractual relationship between customer as defined in the respective Order (“**Customer**”) and **BRYTER GmbH**, Biebergasse 2, 60313 Frankfurt am Main, Germany (“**BRYTER**”) (individually, a “**Party**” and together the “**Parties**”) alongside an Order which references this MSA. Unless defined in the main body of this MSA, definitions are set out in Appendix 1 to this MSA. In the event of conflicts between this MSA and an Order concluded under this MSA, the respective Order shall prevail. The terms of this agreement shall be deemed accepted upon signing an Order.

### 1. Scope of this MSA.

This MSA governs the use of BRYTER’s cloud-based solutions that are provided as part of a subscription, along with any software made available by BRYTER in connection with such services as specified in each Order (the “**Software**”). The Software may include the BRYTER Workflows, BEAMON AI, BEAMON Assist, BEAMON Extract and BRYTER Sandbox, software development kits and APIs made available in connection with such cloud-based solutions. Professional Services may be booked separately.

### 2. Right of Use.

2.1. Subject to this MSA and the respective Order, BRYTER hereby grants Customer (including its Affiliates where so stated in an Order) a limited, non-exclusive, non-transferable right to use the Software during the Subscription Term.

2.2. This MSA is entered into by Customer for and on behalf of itself and its Affiliates (where so stated in an Order). Any such Affiliate shall be entitled to perform any of the obligations and exercise any of the rights of Customer under this MSA, but only Customer shall be entitled to enforce the rights granted to Customer under this MSA, for and on behalf of such Affiliates. Any act or omission of any Affiliate shall be deemed to be an act or omission of Customer. Any loss, damage, liability, costs and expenses incurred by any such Affiliate, shall be deemed to be incurred by Customer. Any such Affiliate may also enter into a separate MSA at any time.

2.3. Where the terms of an Order reference a Trial Period, BRYTER hereby grants to Customer a nonexclusive, nontransferable, revocable right to use parts of the Software during the Trial Period in accordance with the relevant Order.

2.4. Each Authorized User shall have their own individual login and password. Authorized Users may not share their Accounts with other users. An Account may be assigned to another user only where the original user is no longer working for Customer, on a leave of any kind for more than three consecutive months or is no longer carrying out a function that relates to the Software. Authorized Users may only use the Software in accordance with the applicable definitions of the roles assigned to them. BRYTER may, upon reasonable notice, audit Customer’s compliance with the limitations and requirements set out in this 2.4.

### 3. Uptime Commitment and Support.

3.1. BRYTER shall provide Support and ensure uptime of the Software in accordance with the Support & Maintenance Services in Appendix 2.

3.2. Customer Support is included in every paid subscription. Where explicitly stated in an Order, a paid subscription may also include a level of support from our Customer Success team to help with the overall success and adoption of the Software.

### 4. Restrictions on Use

4.1. Customer may only use the Software subject to the Scope as defined in each Order. If at any time during a Trial Period or the Subscription Term, Customer exceeds the Scope, BRYTER shall invoice Customer at BRYTER’s then applicable rates (unless such pro rata pricing is set out in an Order in which case such pricing in the Order shall prevail), based on that increased usage beyond the Scope. BRYTER shall not invoice Customer for exceeding the Scope if BRYTER has not notified Customer when their usage reaches 80% of the Scope providing BRYTER’s standard rates applicable at that time.

4.2. Customer may not (and will not allow any third party to): (i) sell, license, distribute, assign, provide, permit use of or otherwise transfer in whole or in part the Software to another party, except for the purposes of publishing Applications (in relation to BRYTER Workflows); (ii) use the BRYTER Workflows to host Applications on behalf of third-parties to this MSA without BRYTER’s prior written consent; (iii) perform or attempt to perform any actions that would interfere with the proper

functioning of the Software, including but not limited to the circumvention of or interference with any security or other technological feature of the Software; (iv) create derivative works based on the Software; (v) remove or modify any Software markings or any notice of BRYTER's proprietary rights; or (vi) use the Software for any unlawful purposes. Except to the extent expressly permitted under this MSA or applicable law, Customer may not decompile, disassemble, reverse engineer, or otherwise attempt to derive source code from the Software, in whole or in part. For the avoidance of doubt, security testing and scanning of the Software requires written permission by BRYTER.

4.3. Customer agrees that it is liable for the acts and omissions of each Affiliate and each Authorized User, as though those acts and omissions were those of the Customer.

4.4. Customer is responsible for reviewing and validating all results generated by the Software before relying on them for business, legal or other decisions. This applies in particular to results produced by Applications, Modules or Custom Actions configured by or on behalf of Customer. BRYTER warrants the technical functionality of the Software but does not warrant the accuracy of results in any individual case, which depend materially on the respective configuration, underlying data and specifications provided by Customer.

## 5. **Restricted Release.**

If Customer participates in any version of the Software marked as alpha, beta or otherwise designated as a restricted release including but not limited to API releases ("**Restricted Release**"): (i) Customer shall promptly report to BRYTER any error condition discovered in the Restricted Release; (ii) BRYTER shall have no obligation to correct errors or deliver updates to the Restricted Release; (iii) BRYTER shall have no obligation to otherwise support the Restricted Release; (iv) Customer shall provide BRYTER with appropriate test data for the Restricted Release if necessary to resolve problems in the Restricted Release encountered by Customer; (v) the Restricted Release is experimental, may contain problems and errors and is being provided to Customer on an as-is basis with no warranty of any kind, express or implied; (vi) neither Party shall be responsible or liable to the other for any losses, claims or damages of whatever nature, arising out of or in connection with the performance or non-performance of the Restricted Release; and (vii) Customer shall not distribute the Restricted Release to third parties without the prior written consent of BRYTER.

## 6. **BRYTER Workflows only: APIs.**

In the event BRYTER provides Customer with access to the API, the following provisions shall apply:

6.1. BRYTER shall grant Customer a non-exclusive, worldwide, non-transferable, limited license to access the API and its related documentation only as necessary to develop, test and support Customer's own application based on that API. Customer must not (i) sell, rent, lease, sublicense, distribute, or otherwise transfer the API or any portion thereof to any third party; (ii) modify, alter, or create derivative works of the API; (iii) reverse engineer, decompile, or disassemble the API; or (iv) remove or alter any proprietary or confidentiality notices contained in the API.

6.2. The API allows Customer to use the technical infrastructure provided by BRYTER to integrate Applications in Customer's third-party applications in accordance with the applicable Documentation. Customer is solely responsible for any implementation of the API on Customer's side.

6.3. BRYTER may, in its sole discretion, provide Customer with software development kits or code samples (hereinafter jointly referred to as "**Code Samples**"). Code Samples are provided free of charge and are excluded from the paid services provided by BRYTER. Code Samples are provided in electronic form and can be downloaded from a dedicated website. BRYTER is not obligated to develop Code Samples or to keep Code Samples functional or available at all times. Code Samples are not suited for any use in production environments and are provided for educational purposes only.

6.4. BRYTER may introduce new versions of the API with an additional or different range of features. BRYTER may replace deprecated versions of the API provided that the replacement is reasonable for Customer in consideration of the interests of both Parties.

6.5. For purposes of Customer participating in the Restricted Release, Customer may need to disclose code to BRYTER to use the full functionality of Restricted Release ("**Customer Code**"). For the avoidance of doubt BRYTER may not be held liable for any infringement caused by Customer through such Customer Code and Customer is responsible for obtaining all necessary licenses with regards to Customer Code.

## 7. **BRYTER Workflows only: Professional Services.**

7.1. Professional Services can be purchased for the BRYTER Workflows and are subject to a separate SOW and will be performed with due skill, care, and ability in accordance with good industry practice, applicable laws and using appropriately trained personnel.

7.2. The performance of the Professional Services is contingent on Customer (i) meeting any dependencies set out in the SOW, (ii) making decisions and providing information as necessary for BRYTER to be able to provide the Professional Services, and (iii) allowing BRYTER such access to its facilities, equipment and data as is reasonably required to provide the Professional Services.

## 8. Payments.

8.1. Customer shall pay to BRYTER the Fees stipulated in the respective Order in the currency set out therein. Unless stated otherwise in the Order, BRYTER will invoice Customer (a) the Fees relating to the Software annually in advance; and (b) the Fees for any Professional Services as set out in the applicable SOW. All amounts and Fees stated or referred to in this MSA, any Order and SOW are exclusive of all Taxes which Customer shall pay in addition.

### 8.2. Discounts and Special Conditions.

8.2.1 Any discounts, rebates, price reductions, special conditions, complimentary licences or other concessions (together, "**Discounts**") granted in an Order, in connection with a Renewal Term, or in any other agreement between the Parties shall apply exclusively for the period expressly stated in the respective agreement. Where no such period is expressly stated, the relevant Discount shall apply exclusively for the Initial Term or the Renewal Term (as applicable) in which it has been granted, and shall automatically lapse at the beginning of the immediately following Renewal Term.

8.2.2 From the Start Date of any subsequent Renewal Term, the Fees shall be invoiced at BRYTER's then-applicable standard rates, unless the Parties have agreed in writing (email being sufficient) prior to the start of such Renewal Term that the Discount shall continue to apply or be re-granted.

8.2.3 Notwithstanding Sections 8.2.1 and 8.2.2, Discounts the granting of which is conditional upon a particular status or membership of Customer ("**Status Discounts**", e.g. DAV Discount) shall continue to apply for as long as the relevant status or membership is maintained. Customer shall notify BRYTER in writing (email being sufficient) of any lapse of, or change to, the status or membership giving rise to the Status Discount without undue delay, and in any event within thirty (30) days. Upon lapse of the relevant status or membership, the entitlement to the Status Discount shall also lapse, and BRYTER shall be entitled to invoice at standard rates from the billing period immediately following such lapse. BRYTER may, on reasonable prior notice, verify the continued existence of the relevant status or membership or request appropriate evidence from Customer.

8.3. In the case of multiple year Subscription Terms or Renewal Terms in accordance with section 15.2, BRYTER may, on each anniversary of the the start date of the respective Subscription Term, adjust the Fees for the following year ("**Adjustment**") to reflect increases in BRYTER's costs of providing the Software, including but not limited to increases in personnel, infrastructure, or third-party service costs. Any such Adjustment shall be made in good faith, shall be reasonable and proportionate to BRYTER's cost increases, and shall not exceed ten percent (10%) per year unless otherwise agreed in writing by the Parties.

8.4. If Customer's internal processes require a purchase order or purchase order number to be submitted with an invoice, Customer shall provide to BRYTER such purchase order and/or purchase order number with the signed Order. Payment of invoices shall not be delayed or withheld by Customer due to Customer's internal ordering processes or formalities, including the requirement and/or failure to provide a purchase order number.

8.5. By purchasing additional Software services, e.g. Professional Services under a SOW and/or Guided Building and/or BRYTER Virtual Training Program Customer obtains the right to consume the specified amount of purchased sessions within three (3) months after purchase date. After that period, these sessions shall be deemed expired and no longer available for consumption by Customer. Expired sessions cannot be carried over into successive Renewal Terms, cannot be offset against any payment obligations by Customer and BRYTER will not and is not obligated to issue a refund for expired sessions.

8.6. Customer shall pay undisputed invoices by bank transfer within thirty (30) days upon receipt of an invoice. Any Fees not paid when due shall accrue interest at a rate of 6 per cent per annum from the due date until payment is made, whether before or after judgement. BRYTER can deny access to the Software temporarily until overdue payments have been received

(without prejudice to any other rights it may have), provided it has given Customer 15 days' written notice of its intention to do so.

8.7. Customer may withhold payment of particular Fees (or elements of them) that it reasonably disputes in good faith on the basis that BRYTER has not performed in accordance with the terms of this MSA and/or the respective Order. Customer may not withhold payment for any non-disputed element of Fees. Customer must raise such dispute within the time for payment of that invoice, failing which such invoice shall be deemed to be undisputed and no amounts may be withheld.

8.8. Where approved by Customer in advance (including under an Order), Customer will reimburse BRYTER for all reasonable travel, subsistence and other expenses incurred by BRYTER staff and contractors in providing Professional Services to Customer.

## 9. Customer Data.

9.1. Customer shall own all right, title and interest in and to all of the Customer Data and shall have sole responsibility and liability for the legality, appropriateness, accuracy, quality and integrity of the Customer Data. Customer is solely responsible for obtaining any consents required for the use of Customer Data within the Software.

9.2. Customer grants BRYTER a non-exclusive, royalty-free license for a Trial Period and/or Subscription Term (as applicable) to use, host, transmit, display, and create derivative works of the Customer Data solely in connection with the provision of the Software and Professional Services (if applicable).

9.3. Customer agrees not to use or permit the use of the Software to display, store, or process any Customer Data, that may (i) menace or harass any person or cause damage or injury to any person or property; (ii) involve the publication of any material that is false, defamatory, harassing or obscene; (iii) violate privacy rights or promote hatred or harm; (iv) in relation to the BRYTER Workflows constitute unsolicited bulk e-mail or "junk" mail; (v) infringe Intellectual Property rights, or (vi) violate applicable laws. If BRYTER receives information that Customer is in violation of any of the foregoing, BRYTER will notify Customer, and Customer will promptly take appropriate action to resolve such violation. If Customer does not take required action in accordance with the above, BRYTER reserves the right, but has no obligation, to take remedial action, including the removal or disablement of access to such material (without liability on BRYTER's part).

9.4. Customer shall defend BRYTER, or at Customer's option, settle any claim or action brought against BRYTER by a third party alleging that Customer Data violates the provisions of section 9.3 and will indemnify BRYTER for any damages finally awarded against BRYTER by a court of competent jurisdiction or for amounts paid by BRYTER under a court-approved settlement or a settlement of such a claim. The indemnification obligations above are subject to BRYTER providing Customer with prompt written notice of such claim granting Customer sole control of the defense and settlement of such claim; not entering into any settlement or compromise of any such claim without Customer's prior written consent; and providing Customer with all reasonable information for such claim at Customer's expense.

9.5. Customer's rights under Chapter VI of Regulation (EU) 2023/2854 (EU Data Act), in particular with respect to switching providers and the porting or deletion of data, are not restricted by this MSA. The applicable technical modalities and instructions are set out in the [Documentation](#).

## 10. Software Warranty.

10.1. Except as otherwise agreed in this MSA, BRYTER represents and warrants to Customer that during the Subscription Term (i) it has the power to grant Customer the rights set out in this MSA; (ii) the Software will be provided with reasonable skill and care and in compliance with applicable laws, (iii) the Software shall materially conform to the applicable Documentation and respective Order, and (iv) BRYTER shall not materially decrease the functionality of the Software.

10.2. Subject to section 10.3, and notification of such by Customer, if the Software does not comply with the warranty in section 10.1, BRYTER will, at its discretion, use reasonable endeavors to correct such error promptly, or will provide Customer with alternative means of carrying out the task which it was carrying out using the Software.

10.3. BRYTER will not be liable under any warranty or any other provision of this MSA or Order to the extent that any loss or damage is caused by Customer or any Authorized User not having complied with the MSA, the applicable Documentation or Order.

10.4. BRYTER is constantly improving and updating the Software and aims to provide new and innovative features and services. Customer shall always have access to the latest version of the Software. Customer acknowledges that BRYTER may

update or modify certain elements of the Software and introduce new features as BRYTER sees fit, provided that BRYTER shall comply with the warranties set out in section 10.1 for the Subscription Term.

10.5. BRYTER warrants that Deliverables which are provided as a result of Professional Services under a SOW for the BRYTER Workflows and which consist in the provision of a work in accordance with German law (*Werkleistungen*), correspond to the agreed specification and shall remedy Errors in accordance with section 10.2. If BRYTER fails to remedy an Error by the end of an additional time period of length set by Customer in writing, Customer may either request an appropriate reduction of the remuneration for the Professional Service concerned or cancel (*zurücktreten*) the respective Order with respect to the Professional Services. Section 14 shall apply accordingly to any claim for damages caused by any Error.

10.6. In the event that BRYTER: (i) fails to properly provide Professional Services for the BRYTER Workflows which are services (*Dienstleistungen*), or (ii) is in breach of contract which breach does not consist in an Error of the Software or a work, Customer must notify BRYTER in writing and set BRYTER a reasonable time period to properly perform its duty or otherwise remedy the breach. Section 14 shall apply accordingly to any claim for damages caused by any Error.

10.7. Save as expressly provided in this MSA, to the fullest extent allowable by applicable law APIs, applicable documentation and all related components and information are provided on an "as is" and "as available" basis without any warranties (express or implied), conditions, representations or undertakings, made by BRYTER including without limitation any implied warranties of satisfactory quality, fitness for a particular purpose or non-infringement, or arising by course of dealing or performance, or by custom or usage in the trade, all of which are hereby expressly disclaimed.

10.8. This section 10 does not apply to any BRYTER Sandbox access and other services free of charge.

## 11. Confidentiality.

11.1. During the Term of this MSA, each Party shall hold in confidence and not use for any purposes unrelated to this MSA or disclose to any third party (except each Party's employees, agents or contractors who have a need to know and who are subject to confidentiality obligations at least as restrictive as those herein) any Confidential Information of the other Party.

11.2. Either Party may disclose Confidential Information of the other Party: (i) in response to a valid order by a court or other governmental or regulatory body; or (ii) as otherwise required by law; or (iii) as necessary to establish the rights of either Party under this MSA. The receiving Party will promptly give notice to the disclosing Party of such compelled disclosure and allow the disclosing Party to object or to seek a protective order, to the extent legally permitted.

11.3. Except as otherwise authorized or required in furtherance of the purposes of this MSA or any Order, promptly upon a request by the disclosing Party, the receiving Party will destroy (and so certify it in writing) or return to the disclosing Party all Confidential Information and all documents or media containing any such Confidential Information and all copies or extracts thereof provided that the receiving Party shall be permitted to retain copies of any computer records and files containing any Confidential Information which have been created pursuant to automatic archiving and back-up procedures, or retain a back-up copy of such Confidential Information as required by law, or internal compliance policies, in which cases such Confidential Information shall continue to be subject to confidentiality obligations even after termination of this MSA.

11.4. For the avoidance of doubt the permission to retain Confidential Information after termination in accordance with this clause, shall not apply to any Personal Data which shall be governed by the data protection provisions herein.

11.5. Subject to Customer's prior written consent, BRYTER may use Customer's name and logo to refer to Customer as customer or as a reference for marketing purposes.

## 12. AI Terms.

These AI Terms apply to Customer's access and use of any feature(s) or functionality within the Software that are enabled by data models trained by machine learning or enabled by other artificial intelligence functionalities, including integrations to third-party systems ("**AI Service**").

### 12.1. Responsibility for and Ownership of Input and Output.

12.1.1. Customer is solely responsible for all content submitted to the AI Service ("**Input**") and the resulting output ("**Output**"; together, the "**Content**"), and retains ownership of Content, provided that no third-party gains ownership of Content. All Output generated by Customer's use of the AI Service shall, upon creation, be

owned exclusively by Customer, insofar as legally permissible. BRYTER does not guarantee that Output is accurate, complete, original, fair, unbiased, or free from offensive content or errors.

12.1.2. Customer is solely responsible for ensuring that any Input complies with all applicable professional secrecy, confidentiality, or non-disclosure obligations, including but not limited to attorney-client privilege or similar duties under relevant laws and regulations. BRYTER shall have no responsibility or liability for any breach of such obligations resulting from the Customer's use of the AI Service.

12.1.3. For the avoidance of doubt, the Output shall not be viewed as legal advice. BRYTER is no a law Firm, does not practice law and does not give legal advice. Hence, BRYTER does not bear any legal responsibility for the Output or any Information that is derived from the AI Services.

12.1.4. Customer acknowledges that Output may reflect or amplify biases inherent in training data and shall verify and validate all Output prior to any use. Content must comply with applicable laws and agreements, and Customer must ensure a legal basis exists for any Personal Data submitted.

Use of Output without proper human oversight—especially for decision-making or compliance—is at the Customer's own risk. BRYTER disclaims any liability arising from reliance on unverified Output or from neglecting known limitations of AI systems.

12.1.5. Customer acknowledges that the accuracy and reliability of the Output generated by the AI Service may be affected if additional features, such as web search or access to legal sources, are not enabled. In such cases, the AI Service may produce responses that are more likely to contain inaccuracies. BRYTER therefore recommends enabling these features where appropriate to support the generation of more accurate and up-to-date results. The usage of said features remains subject to the provisions of these AI Terms, especially 12.1.1.

## 12.2. **Customer Input Will Not be Used for AI Training.**

12.2.1. BRYTER does not use Customer Content to train the machine learning models. Customer's use of the AI Service does not grant BRYTER any right or license to the Customer Content to train machine learning models.

12.2.2. BRYTER may use data collected from Customer's use of the AI Service when Customer (i) voluntarily provides feedback to BRYTER; or (ii) gives BRYTER its permission.

## 12.3. **Fair Usage.**

12.3.1. BRYTER facilitates equitable and responsible access to its services by restricting services usage and prohibiting misuse and abuse of its services. To ensure that services are used in such a manner that is fair to all users, BRYTER prevents single users from excessively consuming resources, which could negatively impact other users' experience.

12.3.2. Each response of an AI Service consumes a specific number of tokens, which corresponds to the amount of Input processed. To maintain a fair distribution of resources, Customer shall not exceed a limit of 10,000,000 tokens consumed per Tenant per day ("**Consumption Limit**"). The Consumption Limit applies in addition to any other limitations and/or restrictions set out in the MSA and/or the respective Order.

12.3.3. If Customer reaches the Consumption Limit, BRYTER may block further token consumption for the respective day and Tenant, excluding the Customer from using further AI Services within the respective Tenant until the beginning of the next day.

## 12.4. **Usage Restrictions.**

Without derogating from Usage Restrictions included in the MSA, Customer hereby represents and warrants that it will not, nor will it authorize anyone on its behalf, including an Authorized User, to:

12.4.1. mislead any person that the Output generated is human generated;

12.4.2. use the AI Service to generate content that expresses or promotes hate, harassment, or violence, exploits or harms children, encourages self-harm, presents illegal, sexual, political, harmful, false, deceiving or misleading information, misuses Personal Data, contains malware, unsolicited bulk content, ransomware, viruses, or other malicious software;

- 12.4.3. use the AI Service for activities which have high risk of economic harm, for adult content, adult industries, and dating apps;
- 12.4.4. offer tailored financial advice without a qualified person reviewing the information;
- 12.4.5. provide health advice, political campaigning or lobbying;
- 12.4.6. use the AI Service in a way that infringes, misappropriates or violates any third-party rights, including privacy rights, Intellectual Property Rights and confidentiality;
- 12.4.7. reverse assemble, reverse compile, decompile, translate or otherwise attempt to discover the source code or underlying components of models, algorithms, and systems of the AI Service (except to the extent such restrictions are contrary to applicable law);
- 12.4.8. use the AI Service to develop foundation models or other large scale AI models that compete with the AI Service, OpenAI, Azure OpenAI or any other third-party involved in the provision of the AI Service; and
- 12.4.9. use any method to extract data from the AI Service, including web scraping, web harvesting, or web data extraction methods, other than as permitted through the API.

### 12.5. **Limited Applicability of the Support and Maintenance Services.**

- 12.5.1. The applicability of the Support and Maintenance Services regarding the AI Service is limited to the extent that the AI Service may be subject to Downtime, interruptions, and errors without any guaranteed response or resolution time.
- 12.5.2. Customer acknowledges that the use of the AI Service can be restricted by volume limitations.

## 13. **Intellectual Property Ownership.**

13.1. Customer acknowledges and agrees that BRYTER owns all Intellectual Property Rights in the Software, its components, the applicable Documentation, feedback on the Software given by Customer, and BRYTER Data (the “**BRYTER IP**”). Except as expressly stated herein, this MSA does not grant Customer, its Affiliates, any Authorized Users and/or End Users any Intellectual Property Rights or any other rights or licenses in respect of the BRYTER IP.

13.2. BRYTER acknowledges and agrees that Customer and/or its licensors own all Intellectual Property Rights in the Customer Data, Applications and other use cases created by Customer in connection with the use of the Software (the “**Customer IP**”). Except as expressly stated herein, this MSA does not grant BRYTER any Intellectual Property Rights or any other rights in respect of the Customer IP. For the avoidance of doubt such ownership of Customer IP shall not give Customer any rights to access or use the Software or applicable Documentation after the expiry or termination of the respective Order (save that BRYTER shall make the Software available to Customer upon request for a maximum of 30 days post termination solely for the purposes of downloading the Customer Data which is stored on Case Databases).

## 14. **Limitation of Liability.**

14.1. BRYTER shall be liable under the terms of this MSA, any Order and SOW in accordance with the provisions set out in this section:

- 14.1.1. BRYTER shall be liable for damages occurred due to the provision of any Professional Services and/or the Software which BRYTER provides free of charge in accordance with the statutory provisions.
- 14.1.2. Notwithstanding the foregoing, BRYTER shall be fully liable for damages in connection with the provisions of any other services provided under this MSA in the event of intent (*Vorsatz*) and gross negligence (*grobe Fahrlässigkeit*) as well as for damages caused by injury to life, body, or health.
- 14.1.3. In the event of slight negligence (*einfache Fahrlässigkeit*), BRYTER shall be liable only for breaches of a material contractual obligation. A material contractual obligation in the meaning of this provision is an obligation which makes the implementation of this MSA possible in the first place and upon which the contractual partner may therefore generally rely.
- 14.1.4. In the event of section 14.1.3, BRYTER’s liability for any lack of commercial results, indirect damages and loss of profits is excluded.

14.1.5. Liability according to section 14.1.3 shall be limited to typical and foreseeable damages at the time of conclusion of each respective Order or SOW. The Parties agree that the typical foreseeable damage per event shall be limited to the amount set out in the respective Order or SOW, respectively.

14.1.6. The liability for loss of data in the event of section 14.1.3 shall be limited to typical recovery costs which would arise if Customer had made a backup of the relevant data.

14.1.7. Limitations of liability shall also apply to employees, sub-contractors and agents of BRYTER.

14.2. The potential liability of BRYTER for any guarantees or claims based on the German product liability act (*Produkthaftungsgesetz*) remains unaffected.

14.3. Further liability of BRYTER shall be excluded.

## 15. Term and Termination.

15.1. This MSA takes effect on the Effective Date and will remain in effect until all respective Orders and Renewal Orders have expired or been terminated.

15.2. Each Order shall commence on the Start Date. Subject to earlier termination in accordance with sections 9.5, 15.3 or 15.4, the Order will continue for the Initial Term and then for successive Renewal Terms unless terminated by either Party in written notice with a notice period of at least 90 days to the end of the Initial Term or the respective Renewal Term. In the event an Order sets out a Trial Period, the Trial Period shall automatically roll over into the Initial Term unless Customer notifies BRYTER that it wishes to terminate the Order in accordance with the terms of that Order.

15.3. An Order may be terminated by a Party immediately upon notice to the other Party if the other Party (i) becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or creditor assignment or analogous event in any applicable jurisdiction, or (ii) breaches any of its obligations under this MSA and/or the respective Order in any material respect, which breach is not remedied within thirty (30) days following written notice to the breaching Party.

15.4. An Order may also be terminated by Customer immediately on written notice to BRYTER in the event of a Persistent Breach by BRYTER in relation to that Order.

15.5. If Customer exercises its switching or deletion rights under Regulation (EU) 2023/2854 (EU Data Act) and such exercise results in the early termination of an Order, the following shall apply:

15.5.1. Prepaid Fees are non-refundable.

15.5.2. All unpaid Fees for the remainder of the Initial Term – including the remaining portion of the Initial Term and any Renewal Term that has already commenced – shall become immediately due and payable upon the effective date of termination. The calculation shall be based on the Fees agreed in the applicable Order for the entire Initial Term, irrespective of the payment intervals set out therein.

15.5.3. If the acceleration under 15.5.2 is not enforceable in a given case, Customer's obligation to pay the Fees shall continue at the payment intervals set out in the Order as if the Order remained in effect for the full Initial Term.

15.5.4. The foregoing provision for early contract termination is without prejudice to either Party's termination rights under sections 15.3, 15.4 or 15.8.

15.6. Upon termination of this MSA and any Order, Customer shall cease using the Software immediately. Following termination by Customer in accordance with section 15.3 or 15.4, BRYTER shall refund to Customer any fees paid by the Customer in advance in respect of the period following the date of termination. If the Order is terminated by BRYTER in accordance with section 15.3, Customer will promptly pay any unpaid amounts including those covering the remainder of the Subscription Term. In no event will termination relieve Customer of its obligation to pay any fees payable to BRYTER for the period prior to the effective date of termination.

15.7. During the Subscription Term, Customer can access its Customer Data at any time. In regard to the BRYTER Workflows, Customer may perform a final export of Customer Data which is stored on Case Databases before the Subscription Term expires. After the end of the Subscription Term, BRYTER will delete or overwrite the Customer Data remaining on servers hosting the Software unless applicable mandatory law requires retention. Retained data is subject to the confidentiality provisions in this MSA.

15.8. Each Party's statutory rights of termination for good cause shall remain unaffected.

## 16. General.

16.1. **Data Protection.** The Parties acknowledge that all provisions related to applicable data protection laws are set out in a separate data protection agreement which is an addendum to this MSA.

16.2. **Entire Agreement.** This Agreement sets out the entire agreement between the Parties and supersedes any previous agreements between the Parties relating to its subject matter. No terms or conditions contained in a purchase order or any other document or implied course of dealing shall apply to this Agreement. Each Party acknowledges and agrees that it has not relied on any representations made by the other except as set forth in this Agreement. Any such representations are excluded.

16.3. **Waiver.** A waiver of any right under this Agreement is only effective if it is expressed as a waiver and sets out which provision is being waived in writing. It applies only to the Party to whom the waiver is addressed and to the circumstances for which it is given. Unless specifically provided otherwise, rights arising under this Agreement are cumulative and do not exclude rights provided by law.

16.4. **Invalid provisions.** If any provision (or part of a provision) of this Agreement is found by any court or body of competent jurisdiction to be invalid, unenforceable, or illegal, the other provisions shall remain in force. If any invalid, unenforceable or illegal provision would be valid, enforceable, or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the Parties.

16.5. **Governing Law and Jurisdiction.** This Agreement and any disputes or claims arising out of or in connection with it, its subject matter or formation (including non-contractual disputes or claims) will for all purposes be solely and exclusively governed, construed, and enforced in accordance with the laws of Germany. Both parties submit to the exclusive jurisdiction of the courts of Hamburg, Germany.

16.6. **Third Party Rights.** A person who is not a party to the Agreement has no rights to enforce, or to enjoy the benefit of, any term of this Agreement (except as otherwise stated herein).

16.7. **Assignment.** Subject to section 354a German Commercial Code, neither BRYTER nor Customer may assign or otherwise transfer this Agreement or any of its rights or obligations under it to any third party without prior written consent from the other party. Any attempted assignment, or other transfer in violation of this provision shall be void. Nothing in this section shall restrict a party from assigning its rights under this Agreement to any undertaking which acquires its business, provided that such acquiring entity is not a competitor of the non-assigning Party and the assigning Party is not in breach of this Agreement.

16.8. **Force Majeure.** Neither Party shall be in breach of the Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure result from a Force Majeure Event. In such circumstances the time for performance shall be extended by a period equivalent to the period during which performance of the obligation has been delayed or failed to be performed. If the period of delay or non-performance continues for the period of fourteen (14) days, the Party not affected may terminate the Agreement by giving seven (7) days' written notice to the affected Party.

16.9. **Notices.** All notices given under this Agreement (except for notices given pursuant to Appendix 2) must be in writing and sent by pre-paid letter post or by email to the postal or email address for legal notice set out on the Order or to such other postal or email address as may from time to time be notified in accordance with this section, and will be deemed to have been given: if sent by pre-paid letter post, two Business Days after posting; and if sent by email, three Business Hours after being sent to the correct email address (provided the sender has not received notice of failure of delivery). Any notice sent to BRYTER must be copied to [legal@bryter.io](mailto:legal@bryter.io).

16.10. **Variations.** Save as otherwise expressly stated in this Agreement, the terms of this Agreement may only be modified or varied in writing executed by duly authorized representatives of both parties.

16.11. **Survival.** Sections 4 (Restrictions on Use), 11 (Confidentiality), 13 (IP Ownership), 14 (Limitation of Liability), 15.5 (Effect of Termination), and 16 (General) of this Agreement shall survive termination.

## Appendix 1

–

### Definitions

#### General

**“Account”** means each Authorized User’s personal login to the Software.

**„Adjustment“** means an adjustment to the Fees as described in section 8.2.

**“Admin”** means an Authorized User with access to the admin console as set out in the BRYTER Workflows Documentation and, for BEAMON AI, a heightened administrative role with centralized control over user access and core system governance, including elevated troubleshooting capabilities beyond standard user-level controls.

**“Affiliate”** of any Party means any other legally independent entity that directly, or indirectly through one or more intermediaries, is in control of, controlled by, or is under common control with the Party.

**“Agreement”** means the Master Service Agreement, the Definitions, the Data Processing Addendum, the Support and Maintenance Services, the Privacy Policy, any Order and / or Renewal Order referencing the Master Service Agreement, and any auxiliary agreements referenced in an Order as the case may be.

**“AI Content”** means any content, data, or information generated by the AI Service in response to Input provided by Customer or its Authorized Users. Output may include but is not limited to natural language text, summaries, extracted data, or recommendations. For the avoidance of doubt, AI Output is not reviewed, verified, or curated by BRYTER and may be inaccurate, incomplete, or misleading. AI Output is considered part of the Content as defined in Section 12 of this Agreement.

**“AI Service”** means feature(s) or functionality within the Software as described in section 12.

**“API”** means the documented application programming interfaces made available by BRYTER that enable automated interaction with the Software, including access to Exportable Customer Data for purposes of Migration or Deletion in accordance with applicable interoperability standards. Software-specific API endpoints and capabilities are set forth in the applicable Documentation.

**“Authorized User”** means a person at Customer or its Affiliates to whom Customer grants access authorization to use the Software. Admins are always Authorized Users and are also referred to as Authors.

**“BEAMON AI”** means a software-as-a-service solution hosted by BRYTER or its subcontractors that leverages large language models to automate tasks such as contract review, information extraction, content generation, and the interactive resolution of user queries through a conversational interface. Beamon AI is an AI Service within the meaning of Section 12. BEAMON AI includes the two basic features BEAMON Assist and BEAMON Extract.

**“BEAMON Assist”** means a software as a service solution hosted by BRYTER or its subcontractors which automates tasks with the help of large language models. BEAMON Assist is part of BEAMON AI and an AI Service within the meaning of section 12.

**“BEAMON Extract”** means a software as a service solution hosted by BRYTER or its subcontractors which automates contract review and extraction functionality with the help of large language models. BEAMON Extract is part of BEAMON AI and an AI Service within the meaning of section 12.

**“BRYTER Data”** means any information or data provided by BRYTER to Customer as part of the Software and/or Professional Services, together with any feedback from Customer, and Usage Data.

**“Business Days”** means Monday to Friday excepting bank holidays in the location where the contracting BRYTER entity is incorporated.

**“Business Hour”** means any hour on such days in such time zones between 9am and 5pm.

**“Confidential Information”** means non-public information that either Party may obtain from the other or have access to by virtue of the Agreement, including, but not limited to, each Party’s data and each Party’s proprietary software and computer

operations, all code, inventions, algorithms, business concepts, workflow, marketing, financial, business and technical information, the terms and pricing under the Agreement, and all information either clearly identified as confidential or that is of a nature that a reasonable person would understand to be confidential.

**“Consumption Limit”** means the maximum number of tokens that can be consumed in AI Services per Tenant per day within the meaning of section 12.3.2.

**“Customer Data”** means any data provided by Customer (including text, audio, video and images) which BRYTER processes in connection with the provision of access to the Software and/or performance of Professional Services under a SOW and/or Guided Building and/or BRYTER Virtual Training Program.

**“Customer Support”** means the services as described and limited in section 2 and 4 in Appendix 2 (Support and Maintenance Services).

**“Documentation”** means any technical literature or instructions, and other written materials ordinarily provided by BRYTER with regard to the Software.

**“Downtime”** means the total number of minutes during a calendar month for a given functionality of the Software during which that functionality is unavailable, excluding any Excluded Downtime. A minute is considered to be unavailable for a given functionality if all continuous attempts by BRYTER’s monitoring system to write to that functionality within that minute fail. Partial minutes of unavailability will not be counted as Downtime.

**“Effective Date”** means the date on which Customer signs its first Order or any subsequent Order. If signed on separate days, Effective Date means the date of the last signature.

**“End User”** means each person who is authorized by Customer to use the Software without being an Authorized User. For the BRYTER Workflows this means each person who is authorized by Customer to use a Module or an Application and includes both Internal Users and External Users. For BEAMON Assist, this includes only Internal Users.

**“Error”** means a condition which results from the Software materially failing to perform as set forth in the applicable Documentation.

**“Excluded Downtime”** means any minutes of Downtime in any given month of the Subscription Term resulting in whole or in part from any of the following:

- BRYTER or Customer performing Scheduled Maintenance;
- Termination of the MSA;
- Suspension due to overdue payments;
- Factors outside of BRYTER’s reasonable control, including any Force Majeure Event, internet access issues, Downtime resulting from outages, model changes, or any other type of inoperability of Third-Party Services or parts thereof, or related problems;
- Any actions or inactions of Customer or any third party on behalf of Customer;
- Customer’s use of the Software in a manner inconsistent with the applicable Documentation or BRYTER’s guidance;
- Attributable to acts by persons gaining unauthorized access to or use of the Software due to Customer’s failure to maintain and control security and access to the Software; and
- Attributable to the acts or omissions of Customer or its employees, agents, contractors, or vendors, or anyone gaining access to the Software and/or the Support services by means of Customer’s credentials or equipment.

**“External User”** means an End User who does not form part of Customer’s workforce.

**“Fees”** means the consideration payable by Customer to BRYTER for the use of the Software and/or the Professional Services and/or Guided Building and/or BRYTER Virtual Training Program, as defined in the respective Order and/or SOW.

**“Force Majeure Event”** means circumstances beyond a Party’s reasonable control including but not limited to: any strike, lock-out or other industrial dispute; the failure or interruption of a utility service or transport or telecommunications network (including the internet); any act of God, war, riot, civil commotion, malicious damage; compliance with any law or governmental order, rule, regulation or direction; any accident, breakdown of plant or machinery; any fire, flood, storm or other adverse weather condition.

“**Initial Term**” means the first term, commencing on the respective Start Date, during which BRYTER shall grant access to the Software as defined in an Order.

“**Instruction**” means instruction issued by Controller to Processor, directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“**Intellectual Property**” means any patents, patent rights, design rights, copyrights, database rights, trade secrets, know-how, trademarks, trade names, service marks and other intellectual property embodied therein and all applications and rights to apply for registration or protection rights pertaining thereto, in existence on the Effective Date or created in the future. Rights regarding Intellectual Property shall be referred to as “**Intellectual Property Rights**”.

“**Internal User**” means an End User that is employed by Customer.

“**Maintenance Work**” means the development and adaption of the Software by BRYTER in order to improve the Software and/or introduce new functions or eliminate Errors, which may lead to unavailability.

“**Major Error**” means Errors that restrict the use of the Software and for which troubleshooting is urgently needed. This includes a partial loss of the Software with severe impact on the business and where no workaround exists.

“**Order**” means an order form signed by both Parties that references this MSA.

“**Persistent Breach**” means a failure to meet (i) the availability service level set out in section 1 of Appendix 2 more than three times in any period of 3 consecutive months, or (ii) the Support obligations in Appendix 2 more than 3 times in any period of three months.

“**Personal Data**” has the meaning according to Article 4 no. 1 of the General Data Protection Regulation (GDPR).

“**Processing**” has the meaning according to Article 4 no. 2 of the General Data Protection Regulation (GDPR).

“**Professional Secrets**” means data that is subject to professional secrecy obligations (“*Berufsgeheimnis*”) under section 203 of the German Criminal Code or other confidentiality obligations under national law.

“**Renewal Term**” means a period of 12 months beginning on the expiry of the Initial Term or the immediately preceding Renewal Term, as applicable.

“**Response Time**” means the time from the receipt of an incident or Support Request notification to the provision of an initial response by BRYTER.

“**Restricted Release**” has the meaning given to it in section **Error! Reference source not found.**

“**Scheduled Maintenance**” means any repair, maintenance or update to the Software which disrupts the use of the Software. Maintenance will be performed according to the following schedule:

- For EU Cloud Hosting between 10PM (CET) and 5AM (CET) on Wednesdays.
- For US Cloud Hosting between 1AM (EST) and 4AM (EST) on Thursdays.

“**Scope**” means, in relation to the Software, the limitations on usage set out in an Order.

“**Service Availability**” means service uptime of the Software at a standard operating time of 24x7 on 365 or 366 days per year excluding any Excluded Downtime.

“**Session**” means the user interaction with a Live Application, beginning with an End User triggering the start node of a Live Module.

“**SLA**” means the service level agreement attached to this MSA as part of the Support and Maintenance Services set out in Appendix 2.

“**Software**” means all services offered by BRYTER as described in section 1 but excluding Professional Services, Guided Building, BRYTER Virtual Training Program and Support and Maintenance Services.

“**Start Date**” means the start date of the Subscription Term of each respective Order as indicated therein.

“**Sub-processor**” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Controller in connection with the MSA.



“**Subscription Term**” means the duration of an Order for Software, including the Initial Term and any Renewal Term, but excluding the Trial Period.

“**Support and Maintenance Services**” the services specified in [Appendix 2](#).

“**Support Request**” means a question or request from Customer in the Ticketing System that are designated as less critical, for example because Customer’s operations in the Software are minimally impacted, a workaround exists that minimizes impact on Customer’s operations, or Customer wishes to register a request for a new or enhanced feature. A request is processed as Support Request provided that it concerns the functionality of the Software.

“**Taxes**” means any and all applicable sales, value added or withholding tax, or other assessments imposed or collected by any governmental entity worldwide under or pursuant to the MSA (excluding any other taxes that BRYTER is required to pay in its country of incorporation).

“**Team**” means a group of people employed by Customer who perform interdependent tasks to work towards accomplishing a common mission or specific objective. For BRYTER Assist, a Team includes the persons added to the Software as team members and whose access is not limited to asking Questions.

“**Tenant**” means an isolated share of the Software. It offers user access and authorization management, data storage and configuration.

“**Third-Party Services**” means software not manufactured by BRYTER that is either implemented in the Software or provided together with the Software.

“**Ticketing System**” means Customer sending a Support Request in English via e-mail to: support@bryter.io.

“**Trial Period**” means the trial period defined in an Order during which Customer may test the Software.

“**Usage Data**” means anonymized information collected by BRYTER in relation to Customer’s and End Users’ use of the Software (including analytics, data and insights).

### BRYTER Workflows

In addition to the general definitions above, the following definitions apply to licenses of the BRYTER Workflows.

“**Additional Features**” means any feature that BRYTER has agreed to provide to Customer in accordance with the terms of an Order or which Customer has decided to purchase and which is not necessarily included in the BRYTER Workflows (without an Order) and which are listed [here](#).

“**AI Connector**” means the set of nodes which perform actions with the help of large language models and is used within a module.

“**Application**” means a set of one or several Module(s), case databases, data views and further software functionalities (as applicable) that can be combined to create a solution for one specific use case or larger purpose and is built by Authorized Users except when Building Services are expressly set out in a separate SOW.

“**Author**” means a specific and personalized login and password ascribed to an Authorized User who may use the BRYTER Workflows to build and publish Live Applications and Live Modules.

“**Authorized User**” means a person at Customer or its Affiliates to whom Customer grants access authorization to use the BRYTER Workflows. Admins are always Authorized Users and are also referred to as Authors.

“**Basic Features**” means any functionality of the BRYTER Workflows including but not limited to different types of input, value and action nodes excluding any Additional Features.

“**BRYTER Workflows**” means the solution hosted by BRYTER or BRYTER’s subcontractors and made available as a software as a service (SaaS), including Additional Features where these have been purchased by Customer, and including any developments to such product resulting from the provision of Professional Services. BRYTER reserves the right to add new Additional Features without a respective Order. Such Additional Features will not become part of the license unless expressly specified in Customer’s respective Order. For the avoidance of doubt, the BRYTER Workflows is fully functional without Additional Features.

“**BRYTER Workflows Documentation**” means guidelines, instructions and recommended actions for the BRYTER Workflows available [here](#).

“**BRYTER Connect**” means services that allow for the connection to the BRYTER Workflows from other systems through APIs and the possibility for Customer to create additional functions in Modules and Applications (“**Custom Actions**”). The functionalities and limitations of BRYTER Connect are outlined in the BRYTER Connect documentation hub (<https://developer.bryter.io/>). Customer is solely responsible for any implementations of the Custom Actions running in its Applications.

“**BRYTER Multi-Client**” means the Additional Feature through which Customer can build and maintain an Application once, and make it available to multiple clients. Each client will have a separate environment with separate users and data, and the Application can be themed differently.

“**BRYTER Multi-language**” means the Additional Feature through which you can deliver multi-language Applications by building Modules and (automatically) translating their contents into different languages.

“**BRYTER Sandbox**” means that Customer may build Test Applications on the BRYTER Workflows. Customer is not allowed to publish Applications and/or Modules to the live environment.

“**BRYTER Virtual Training Program**” means a virtual training service provided by BRYTER to enable Authors to use all Basic Features for building and maintaining Applications on BRYTER Workflows.

“**Building Services**” means services using the Software to create solutions tailored to Customer's needs.

“**Case Database**” means a configurable data storage as part of an Application with the primary purpose to collect and store case records in order to reuse and inter-connect them for further purposes.

“**Components**” means collectively, the automation features and workflow features of the Software.

“**Customer Success**” means additional help through a customer success manager. Customer success activities performed by BRYTER are tailored to each Customer and may include the following: (i) onboarding planning; (ii) regular check-ins; (iii) goals and metrics tracking; (iv) service coordination and oversight; (v) adoption and success plan design; for the avoidance of doubt, this does not include instructor-led workshops, training sessions or Building Services if not specified otherwise in the Order Form or a separate SOW.

“**Deliverables**” means all Building Services, goods, records, reports, documents, papers and other materials (in documentary, electronic or other form) produced or to be produced by or on behalf of BRYTER for Customer as part of the Professional Services pursuant to the execution of a SOW.

“**Document Template**” means a file that serves as a starting point to create a Document Type and that can be uploaded within a “Create Document” node within the BRYTER Workflows.

“**Document Type**” means a specific type of document for a specific use case (i.e., NDA, Employment Contract).

“**Guided Building**” means educative help offered to Customer in building their Applications with the intention of enabling Customer to autonomously design and build Applications. For the avoidance of doubt Customer remains responsible for the completion, functionality and maintenance of the Application and BRYTER does not owe specific Deliverables nor completion of such Application. Guided Building can be purchased via e-mail ([support@bryter.io](mailto:support@bryter.io)) and will be invoiced up-front upon purchase at the then applicable rate communicated upon the purchase request.

“**Internal Live Application**” means a Live Application that can only be used by an Authorized User or an Internal User. Any other Live Application shall be a “**External Live Application**”.

“**Live Application**” means an Application in which at least one Module has been published to the live staging environment by an Authorized User using the publishing feature of the BRYTER Workflows. Any other Application shall be a “**Test Application**”.

“**Live Module**” means a Module which has been published to the live staging environment by an Authorized User using the publishing feature of the BRYTER Workflows. Live Modules are part of a Live Application. Any other Module shall be a “**Test Module**”.



“**Module**” means a single workflow or process built on the BRYTER Automation Platform which consists of an undefined number of nodes that form a single, independent and executable unit always beginning with a start node and ending with a result node.

“**Pages**” means flexible and responsive dashboards, entry pages, and other kinds of user-facing pages, consisting of charts, KPIs, and other content built by Authors.

“**Professional Services**” means the customization, Application development, implementation and/or training services provided on the basis of a project scope defined in a separate SOW and will be invoiced separately monthly in arrears. Each day of Professional Services includes up to 8 business hours.

“**SOW**” means a statement of work, detailing the Professional Services to be provided by BRYTER and paid for by Customer.

“**Test Author**” means a specific and personalized login and password ascribed to an Authorized User who may only use the BRYTER Workflows for the purposes of testing and for training/workshop formats, not for publishing Live Modules and Live Applications.

## Appendix 2

-

### “Support and Maintenance Services”

#### 1. Definitions.

The capitalized terms used in this Appendix shall have the meaning as set forth in the Definitions (Appendix 1) to the MSA.

#### 2. Scope

Subject to each of the other provisions of the MSA, with the purchase of the Software, BRYTER will provide the following Support and Maintenance Services during the applicable Subscription Term:

- i. support Customer with questions concerning the use of the Software in the process of development and in the operation of Applications;
- ii. make available new versions of the Software as outlined below; and
- iii. respond to Support Requests.

#### 3. Customer’s responsibilities

Customer acknowledges that its cooperation is essential to the proper performance of Support and Maintenance Services by BRYTER. To enable BRYTER to provide Support and Maintenance Services, Customer agrees to the following:

- i. If an Error occurs, Customer will promptly inform BRYTER via the Ticketing System;
- ii. The Error must be reproducible by BRYTER without using a special, adapted or extended version of the Software. If necessary, Customer agrees to assist BRYTER in reproducing the Error. Should such a reproduction be impossible, the Error will be described by Customer as precisely as possible;
- iii. If an Error is reported, Customer will (a) provide BRYTER with the information requested to eliminate the problem and support BRYTER in eliminating the Error; and (b) inform BRYTER of any modifications it has made to its usage of the Software, or any other issues of which Customer is aware of; and
- iv. Unless it is commercially unreasonable to do so, Customer will implement suggestions from BRYTER on elimination of Errors.

#### 4. Excluded services

Support and Maintenance Services under the MSA do not include and/or apply to any of the following:

- i. Support and maintenance services on Customer’s infrastructure and/or premises;
- ii. Development of software programs that have other functions than those described in the applicable Documentation;
- iii. Programming services to integrate the Software with products of Customer or Third Parties;
- iv. Support and maintenance services in relation to Downtime resulting from outages, model changes, or any other type of inoperability of Third-Party Services or parts thereof;
- v. Support of adaptations and extensions of the Software programmed by Customer;
- vi. Support and Maintenance Services do not apply to the AI functionalities integrated into the Software (including BEAMON AI), particularly in cases of model changes, token consumption limits, hallucinated output, and probabilistic behavior of LLMs. No guaranteed response or resolution time applies to AI Service-related functionality;

- vii. Support in connection with the enforcement of token consumption limits or consequences of reaching such limits is excluded from Support and Maintenance Services;
- viii. Introduction and training of Customer's employees in the use of the Software;
- ix. Recommendation of action for the optimal use of the Software;
- x. Error correction and consulting services in case of operational Errors that are based on non-compliance with the operating conditions for the Software contained in the applicable Documentation;
- xi. Developing use cases and/or Applications for Customer, or answering questions on these use cases and/or Applications architecture;
- xii. Customized work already covered by a separate SOW;
- xiii. Debugging Applications and/or Modules;
- xiv. Answering questions about BRYTER's roadmap;
- xv. Any Software provided free of charge, including but not limited to access to the Sandbox.
- xvi. BRYTER Virtual Training Program, Guided Building and Professional Services;
- xvii. Any other services not specifically set forth herein, including, but not limited to, customization, programming, integration, recovery of data, support of Customer-specific adaptations or add-on programs and program components, support of modifications, installation, training, analysis or corrections of Errors caused by Customer's non-compliance with this Agreement or Documentation or unauthorized modifications.

## 5. Ticketing System and Service Availability

- i. Subject to each of the other provisions of the MSA, with the purchase of the Software, BRYTER will respond to queries submitted through the Ticketing System regarding Errors and Support Requests using commercially reasonable efforts.
- ii. BRYTER will use commercially reasonable efforts to ensure a Service Availability of 99.5% per month for the Software.
- iii. The use of AI Services is subject to daily token consumption limits as defined in the Master Service Agreement. If a Customer exceeds the daily consumption limit of 10,000,000 tokens per Tenant, BRYTER may restrict further access to the AI Services for that Tenant until the next calendar day. Such restrictions do not constitute Downtime and are excluded from the Service Availability calculation.

## 6. Disaster Recovery

### i. Definitions

For the purposes of this section 6:

**"Recovery Point Objective"** or **"RPO"** means the maximum tolerable period of time during which Customer Data may be lost due to a major incident or disaster, measured from the point of the last successful backup to the point of failure.

**"Recovery Time Objective"** or **"RTO"** means the maximum tolerable period of time between the occurrence of a major incident or disaster and the restoration of the affected functionality of the Software to a state that allows Customer to resume normal operations.

**"Disaster Recovery Event"** means an unplanned outage of the Software that is not an instance of Excluded Downtime and that results in a complete loss of availability of the Software for all Authorized Users and End Users on the affected Tenant.

### 6.2. Recovery Objectives

#### ii. Recovery Objectives

BRYTER shall use commercially reasonable efforts to maintain disaster recovery capabilities for the Software that meet the following targets:

Metric	Target
Recovery Point Objective (RPO)	24 hours
Recovery Time Objective (RTO)	48 hours

The RPO and RTO targets set out in this section 6.ii. represent BRYTER's operational objectives. BRYTER shall design, implement and maintain its backup and disaster recovery infrastructure so as to be capable of meeting these targets under reasonably foreseeable disaster scenarios.

**iii. Scope and Exclusions**

- a. The recovery objectives in section 6.ii. apply to the core functionality of the Software as described in the applicable Order, including the storage and availability of Customer Data.
- b. The recovery objectives in section 6.ii. do not apply to:
  - i. AI Services (including BEAMON AI, BEAMON Assist and BEAMON Extract), which are subject to the limitations set out in sections 4.vi., 4.vii. of this Appendix and 12.5 of the MSA respectively;
  - ii. Third-Party Services or any functionality dependent on the availability of Third-Party Services;
  - iii. any Excluded Downtime as defined in Appendix 1 (Definitions);
  - iv. Professional Services, Guided Building, BRYTER Virtual Training Program and BRYTER Sandbox; and
  - v. any Custom Actions or integrations developed by or on behalf of Customer.

**iv. Backup**

BRYTER shall maintain automated backups of Customer Data at intervals consistent with the RPO set out in section 6.ii. Backups shall be stored in a geographically separate location from the primary production environment within the applicable hosting region (EU or US, as set out in the respective Order).

**v. Disaster Recovery Testing**

BRYTER shall test its disaster recovery procedures at least once per calendar year. Upon Customer's written request (no more than once per calendar year), BRYTER shall provide Customer with a written summary of the most recent disaster recovery test, including the date of the test and whether the RPO and RTO targets were met.

**vi. Notification**

In the event of a Disaster Recovery Event, BRYTER shall:

- a. Notify Customer without undue delay, and in any event within 4 Business Hours of becoming aware of the event, via the contact details set out in the applicable Order;
- b. provide regular status updates at intervals of no less than every 4 hours until the affected functionality has been restored; and
- c. following restoration, provide Customer with a written incident report within 10 Business Days, including the root cause (to the extent known), the duration of the outage, the actual recovery point and recovery time achieved, and the measures taken to prevent recurrence.

**vii. Persistent Breach**

For the purposes of the definition of "**Persistent Breach**" in Appendix 1 (Definitions), a failure by BRYTER to meet the RTO set out in section 6.ii. in connection with a Disaster Recovery Event shall count as a failure to meet the availability service level referred to in Appendix 1.

**viii. Relationship to Service Availability**



Downtime resulting from a Disaster Recovery Event shall be included in the calculation of Service Availability under section 5.ii of this Appendix, subject to the exclusions set out in the definition of Excluded Downtime.

**DATA PROCESSING ADDENDUM**

between

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

and

**BRYTER GmbH**, Biebergasse 2, 60313 Frankfurt am Main, Germany (hereinafter „**Processor**“)

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

IMPORTANT NOTICE: This data processing addendum ("**DPA**") contains, in Section 8, supplementary provisions to ensure compliance with professional secrecy and confidentiality obligations, in particular pursuant to Sections 43a and 43e of the German Federal Lawyers' Act (Bundesrechtsanwaltsordnung, BRAO), Sections 18 and 26a of the German Federal Notary Code (Bundesnotarordnung, BNotO) and Section 203 of the German Criminal Code (Strafgesetzbuch, StGB), to the extent that the Controller is subject to such obligations. Where, in the context of this DPA, personal data are processed that at the same time constitute professionally protected confidential information within the meaning of the aforementioned provisions, the provisions of this DPA relating to the protection of personal data shall apply on a supplementary basis, insofar as and to the extent that they are compatible with the applicable professional secrecy and confidentiality obligations. In the event of any conflict or inconsistency, Section 8 of this Data Processing Addendum shall prevail.

### **1. Definitions**

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.

### **2. General provisions**

- 2.1 Unless otherwise implied (e.g. by context of a reference, or explicitly stated), "**GDPR**" refers to both the EU General Data Protection Regulation as well as the UK General Data Protection Regulation.
- 2.2 Controller is the controller according to Article 4 no. 7 GDPR. Processor is the processor in accordance with Article 4 no. 8 of the GDPR.
- 2.3 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 "**MSA**") according to Art. 4 no. 2 and Art. 28 GDPR solely based on this DPA.
- 2.4 The subject-matter of the Processing is set out in the MSA.
- 2.5 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)	<ul style="list-style-type: none"> <li>• Authorized Users</li> <li>• End User, if a login is required</li> </ul>	<ul style="list-style-type: none"> <li>• Functionality and security</li> <li>• Access control</li> </ul>	Until termination of MSA
Authentication and access credentials (e.g. password hash, login credentials)	<ul style="list-style-type: none"> <li>• Authorized Users</li> <li>• End User, if a login is required</li> </ul>	<ul style="list-style-type: none"> <li>• Functionality and security</li> <li>• Access control</li> </ul>	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)	<ul style="list-style-type: none"> <li>• Authorized Users</li> <li>• End User, if a login is required</li> </ul>	<ul style="list-style-type: none"> <li>• Functionality and security</li> <li>• Service monitoring</li> <li>• Error analysis</li> <li>• Audit logging and compliance</li> </ul>	For security/audit logs up to 90 days where applicable, otherwise until termination of MSA
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)	<ul style="list-style-type: none"> <li>• Authorized Users</li> <li>• End User</li> <li>• Data subjects identifiable with Customer Content (e.g. Customer's employees who are not End Users, business partners of Customers, Customer's clients)</li> </ul>	<ul style="list-style-type: none"> <li>• Provision of the Software and AI Services on Controller's documented instructions</li> <li>• Storage, display, transformation and transmission as required by the Software's functionality</li> <li>• 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</li> </ul>	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.

#### **4. Scope and Responsibility**

Processor shall process Personal Data on behalf of Controller. Such Processing shall include such 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" in accordance with Article 4 no. 7 of the GDPR).

#### **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 regulations.
- 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 and who is obliged to maintain confidentiality, can verify the compliance with the Processor's obligations laid down in the applicable data protection laws and regulations 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 applicable data protection laws and regulations.

- 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 section 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.

## **6. Processor's obligations**

- 6.1 Processor processes Personal Data solely within the scope the MSA and this DPA and on documented instructions of Controller, unless otherwise required to do so by 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 according to Art. 12 to 22 GDPR by Controller.
- 6.3 Taking into account the nature of processing and the information available to Processor, Processor shall assist Controller in its obligations under Art. 32 GDPR as well as its obligation to carry out a data protection impact assessment and prior consultation, where necessary (Art. 35, 36 GDPR). 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 law of the European Union or a member state or the UK.
- 6.5 Where Controller uses functionalities based on large language models as part of the BRYTER Software, Processor shall not be responsible for the accuracy, reliability, or legal validity of any output generated. Such output ("AI Output") is generated automatically based on Controller's Input, and the Controller remains solely responsible for reviewing, validating, and using such Output in compliance with applicable laws. Processor does not process AI Output on behalf of Controller unless it contains Personal Data within the meaning of the GDPR.

**7. Processor's notification obligations**

- 7.1 Processor shall immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other European Union, member state or UK data protection regulations. 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. Processor will inform Controller about damages and costs claimed against him and will not acknowledge claims of third parties without the consent of Controller and will conduct the defense at the discretion of Processor in due collaboration with Controller or leave it to Controller.
- 7.2 Taking into account the nature of processing and the information available to Processor, Processor shall assist Controller regarding Controller's obligations according to Art. 33 and 34 GDPR.
- 7.3 Controller shall pay for any non-insignificant costs incurred by making use of Processor's obligation to support Controller according to section 7.2 as far as the obligation does not arise due to a violation of data protection law by Processor.

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

- 8.1 This section only applies if Controller is subject to professional confidentiality obligations, in particular as a solicitor or member of a legal or tax advisory profession in accordance with Sections 43a, 43e BRAO, as a notary subject to comprehensive official confidentiality obligations pursuant to Section 18 BNotO and Section 203 of the German Criminal Code (Strafgesetzbuch, StGB).
- 8.2 Under the MSA and this 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 obtaining knowledge of Professional Secrets to the extent strictly necessary for the performance of the obligations set out in the MSA including this 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.

- 8.7 Processor acknowledges that in cases where Controller is subject to Section 203 StGB, any unauthorized disclosure of Professional Secrets may constitute a criminal offense under Sections 203 and 204 StGB. Processor shall inform its employees, agents and Sub-processors involved in the processing of Professional Secrets about the criminal liability resulting from unauthorized access to or disclosure of such information.
- 8.8 Where the Controller qualifies as a holder of professional secrecy rights within the meaning of Section 53a of the German Code of Criminal Procedure (Strafprozessordnung, StPO), any Professional Secrets processed under this DPA may be subject to the right to refuse testimony pursuant to Section 53a StPO and to protection against seizure, in particular under Section 97(2) StPO. In the event of any governmental interview, inquiry, or measure aimed at the disclosure or surrender of such information, Processor shall, to the extent legally permissible, object to such request and shall notify Controller without undue delay so that Controller can determine how to proceed.

## **9. Sub-processors**

- 9.1 By signing this DPA, Controller authorizes Processor's use of Sub-processors listed in Schedule 1. Depending on the services outlined in the Agreement, Processor will use different Sub-processors.
- 1.1 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.
- 9.2 Controller shall be entitled to object to any change notified by Processor within 15 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.
- 9.3 Processor shall contractually ensure that Processor's obligations agreed on in this DPA also apply to all approved Sub-processors.
- 9.4 Processor shall remain liable to Controller for its Sub-processors' obligations.
- 9.5 Controller agrees with execution of this DPA to the use of Amazon Web Services (AWS) EMEA SARL ("**AWS**") and Microsoft Azure as a Sub-processor. 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.

9.6 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 member states of the European Union, in another state that is a party to the Agreement on the European Economic Area (“EEA”) or the UK. Subject to compliance with the provisions of this DPA, Processor is also permitted to process Personal Data outside the EEA and UK or to have it processed by Sub-processors in accordance with Section 9 of this DPA, if the conditions of Articles 44 to 48 GDPR are fulfilled or an exception in accordance with Art. 49 GDPR exists.

#### **11. Technical and organizational measures according to Art. 32 GDPR**

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 according to Art. 32 GDPR listed in Schedule 2 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, delete in accordance with data protections regulations, 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 laws of the European Union, of a member state or of the UK 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 deletion of Controller’s data from such backup copies is not technically feasible with regard to Art. 32 GDPR. Notwithstanding

Section 2.5., 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 on 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 GDPR.
- 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.

**Schedule 1**

-

**List of Sub-processors**

<b>Sub-processor</b>	<b>Service Provided</b>	<b>Corporate Location</b>	<b>Server Location</b>
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 (Germany)
DeepL SE	Translation tool (add on)	Maarweg 165, 50825 Köln, Germany	Germany and Sweden
DataDog Inc.	Monitoring Tool	620 8 <sup>th</sup> Avenue, 45 <sup>th</sup> Floor, New York, NY 10019-1741, USA	Frankfurt am Main (Germany)
Microsoft Azure	Cloud Server	Takeda Ireland Ltd (Grange Castle), New Nangor Road, Grange, Dublin 22, Ireland	Central-Gavle (Sweden) Schiphol (Netherlands)
AlphaAI Technologies Inc. dba Tavily	API-based Web Search Processor	33 W 60 <sup>th</sup> St, New York, NY 10023, USA	USA



## 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 European 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.

## **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 AWS and/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 pursuant to 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.



## Privacy Policy

We, BRYTER GmbH (hereinafter “we” or “BRYTER”) are pleased about your interest in our company.

We take the protection of your personal data and their confidential treatment very seriously. The processing of your personal data takes place within the framework of the legal provisions of the data protection law of the European Union, in particular the General Data Protection Regulation (hereinafter “GDPR”) and further applicable regulations.

With this privacy policy, we inform you about our approach to privacy by explaining why and how we process your personal data and explaining your rights. This privacy policy applies to all situations in which BRYTER processes your personal data. This implies visiting the BRYTER websites (bryter.com and beamon.bryter.com), using all BRYTER products such as the BRYTER Platform, BRYTER Assist, and BRYTER Extract, and other situations mentioned in this privacy policy.

If you are in a contractual relationship with BRYTER and a Data Processing Addendum (“DPA”) has been concluded between you and BRYTER, the DPA applies in addition to this privacy policy. The BRYTER DPA can be found [here](#).

### 1. General information

#### 1.1. Controller and contact details

This data privacy policy shall apply to data processing activities by the following controller:

BRYTER GmbH  
Biebergasse 2  
60313 Frankfurt am Main  
E-Mail: [privacy@bryter.io](mailto:privacy@bryter.io)

Legal representatives: Michael Grupp, Dr. Micha-Manuel Bues, Michael Hübl, to be reached under the above contact details.

#### 1.2. Data protection officer

The operational data protection officer can be reached as follows:

# **BRYTER**

HeyData GmbH

Schützenstr. 5

10117 Berlin

E-Mail: [info@heydata.eu](mailto:info@heydata.eu)

## **1.3 Affiliates of the controller**

BRYTER US Inc.

33 Irving Place

Suite 5007

New York, NY 10003, USA

BRYTER Services UK Limited

21-33 Great Eastern St.

London EC2A 3EH, UK

## **2. Subject matter of data protection**

The subject matter of data protection is personal data. This means any information relating to an identified or identifiable natural person ('data subject'). These include e.g. information such as name, postal address, e-mail address or telephone number.

Specific information on the personal data processed by us can be found below in detail in the data processing operations listed.

## **3. Collection and storage of personal data as well as the nature and purpose of their processing**

### **3.1 When visiting the website**

When visiting and using our website, the browser used on your end device will automatically send information to the server of our website. This information is temporarily stored in a so-called log file.

#### **Categories of personal data processed:**

- internet protocol address of the requesting computer
- date and time of the access
- website that is viewed
- browser used

## **Purposes of processing:**

- ensuring smooth establishment of the website's connection
- ensuring comfortable use of our website
- evaluation of system safety and stability, as well as
- other administrative purposes

## **Legal basis:**

- Art. 6(1)(f) GDPR (legitimate interest in operating and securing the website)

Further information on cookies and similar technologies can be found in Sections 6 and 7 of this privacy policy.

## **3.2 Customer Relationship Management**

We offer you the option to contact us via email to purchase access to the BRYTER platform. If you will enter or have entered a customer relationship with BRYTER, we process personal data to manage and maintain our business relationship.

### **Categories of personal data processed:**

- Identification and contact data (e.g. name, email address)
- Contractual and communication data (e.g. emails, service requests, invoices)
- Customer account and usage-related information:

## **Purposes of processing:**

- Customer acquisition and relationship management
- Contract initiation, performance and administration
- Customer support and service fulfillment

## **Legal basis:**

- Art. 6(1)(f) GDPR (legitimate interest in managing customer relationships)
- Art. 6(1)(b) GDPR, where processing is necessary for the performance or initiation of a contract

## **3.3 Meeting Documentation and Transcription**

In the context of sales, customer success, onboarding or similar customer interactions, we may use external meeting documentation tools (e.g. AI-based meeting assistants) to create transcripts, summaries and notes of meetings.

### **Categories of personal data processed:**

# **BRYTER**

- Audio recordings and transcripts of meetings
- Meeting metadata (e.g. participants' names, email addresses, meeting ID, date and time)
- Meeting chat content, where applicable
- If recording is enabled: video and screen-sharing content as part of the meeting recording

## **Purpose of processing:**

- Documentation of meetings (transcripts, summaries, action items)
- Internal quality assurance and follow-up of customer interactions

## **Important clarification on AI usage:**

- Personal data processed in this context is not used to train or improve general AI or machine-learning models.
- AI-based processing is limited to the generation of meeting transcripts, summaries and related documentation for our internal purposes.

## **Legal basis:**

- Art. 6(1)(f) GDPR (legitimate interest in efficient documentation and quality assurance of customer communication)
- Art. 6(1)(b) GDPR, where meetings are necessary for the performance or initiation of a contract
- Art. 6(1)(a) GDPR (consent), where required by applicable law, in particular for audio, video or screen recordings

## **Recipients and roles:**

- External providers of meeting documentation services (e.g. Glyphic) act as processors on our behalf in this context.
- These services are not part of the provision of the BRYTER Software as a Service to customers and are used exclusively within BRYTER's own responsibility (e.g. sales and customer success).

## **Data retention:**

- Meeting recordings and transcripts are retained only as long as necessary for the above purposes and can be deleted or restricted at any time; recordings are deleted in accordance with our internal retention policies.

## **Screen sharing:**

- Screen-sharing content is only captured if meeting recording is enabled. Without active recording, screen-sharing content is not persistently stored.

### **3.4 Payments and Billing (Self-Service Credit Card Payments)**

If you purchase our services via self-service (e.g. by credit card), we process personal data for the purpose of payment processing and billing.

#### **Categories of personal data processed:**

- Identification and contact data (e.g. name, email address, billing address)
- Payment and transaction data (e.g. transaction ID, payment status, amount, currency; credit card data is processed in tokenized form)
- Device and usage data for fraud prevention and security purposes

#### **Purposes of processing:**

- Processing payments and billing
- Fraud prevention and ensuring payment security
- Compliance with legal accounting and retention obligations

#### **Legal basis:**

- Art. 6(1)(b) GDPR (performance of a contract)
- Art. 6(1)(f) GDPR (legitimate interest in secure and efficient payment processing and fraud prevention)
- Art. 6(1)(c) GDPR (compliance with legal obligations)

#### **Recipients:**

- Stripe and affiliated companies, acting as independent controllers for payment processing and fraud prevention. Further information can be found in Stripe's privacy policy.

#### **Data retention:**

- Payment-related data is retained in accordance with statutory retention obligations; otherwise, data is deleted once it is no longer required for the above purposes.

#### **International data transfers:**

- Where data is transferred to third countries, this is done under appropriate safeguards as described in Section 5 of this privacy policy (e.g. EU-US Data Privacy Framework, Standard Contractual Clauses).

### **3.5 Subscribing to our Newsletter**

If you have consented pursuant to Art. 6(1)(a) GDPR, we process your personal data to send our newsletter.

**Categories of personal data processed:**

- Email address
- Name, surname and company affiliation

**Purpose of processing:**

- Sending newsletters and product-related information

**Legal basis:**

- Art. 6 (1) (a) GDPR (consent)

You may revoke your consent at any time for the future.

### **3.6 When using our contact form, email contact or downloading content**

You may contact us via contact forms or email and download content such as guides or reports.

**Categories of personal data processed:**

- Identification and contact data (e.g. name, email address)
- Company affiliation and job title
- Communication content

**Purposes of processing:**

- Responding to inquiries
- Providing requested content
- Occasional informational updates on our products and services

**Legal basis:**

- Art. 6(1)(f) GDPR (legitimate interest in responding to inquiries)
- Art. 6(1)(a) GDPR (consent), where required

### **3.7 Recruitment and Onboarding**

We collect application relevant documentation provided by the candidate. In general, it includes name, surname, e-mail address, address, phone number, a cover letter and the CV and a link to the applicant's LinkedIn profile or website. Moreover, certain information can be provided for self-identification under local US law (gender, race or ethnicity, veteran status, disability). Do disregard this section unless it is required by local law.

# **BRYTER**

Depending on whether your application is successful, we need further information to enter into an agreement/employment relationship with you. This may be: date of birth, bank account details, insurance number, work permits, disabilities if legally required under local law etc. We will also conduct automated checks against applicable sanctions-party lists.

Please do not include in your CV and cover letter information about political opinions, religious beliefs, and similar sensitive data. They are not required for your application.

The legal basis for data processing activities during the recruitment process is the respective national employment law or Art. 6 (1)(b) GDPR (i.e., the processing is necessary for entering into or the performance of a contract with you).

If you provide any information in relation to e.g. referees, you are responsible for obtaining their consent and ensuring that they are aware that their details can be forwarded.

Where we obtain publicly available information about you from business- and employment- oriented social networks or websites, the legal basis is Art. 6(1)(f) GDPR. Our legitimate interests follow from the fact that we wish to conduct a proper assessment of an applicant.

When we do a video interview with you it might happen that we ask for a recording. We will always ask for your consent whether to record or not, pursuant to Art. 6(1)(a) GDPR. Please note – whether you consent is totally up to you. You have the right to revoke your consent at any time without reasons with effect for the future.

BRYTER uses the applicant tracking system & recruiting software Teamtailor for its hiring process. It is used to coordinate the application process, to monitor the status of applications and to communicate with candidates and within the team. Only BRYTER employees who are involved in the application process for the respective position have access to the candidate's data. We have a specific Cookie policy for Teamtailor which can be found [here](#).

The applicant data will be deleted by us six months after the end of the respective application procedure. This is necessary for the burden of proof in the event of a legal claim based on the German General Equal Treatment Act (AGG).

## **3.8 BRYTER Academy & BRYTER Open**

BRYTER's learning platform for students - BRYTER Academy - enables us to provide online courses and learning material to interested participants. Personal data

# **BRYTER**

collected during the onboarding process and course participation is: name, email address, courses, interaction time, login times, progress.

The legal basis for the processing of participants' data is Art. 6(1)(b) GDPR.

BRYTER Open gives non-profits, NGOs and academic institutions the power of our platform for free. If you are using these services, our Customer relationship management section applies to the data collected as well as further privacy information provided on the signed-up service.

## **3.9 In-app behavior analytics**

### **Categories of personal data processed:**

- In-app usage and behavioral data within our platform (e.g., click paths, page and feature usage, session metadata, timestamps)
- Technical identifiers and device information (e.g., browser/device type, operating system, pseudonymous user IDs)
- No customer-generated content, prompts, documents, or attachments from our AI products are transmitted to Userpilot, Inc.

### **Purposes of processing:**

- Product analysis and improvement, UX optimization, feature adoption analysis, and supporting user-centric development of the platform

### **Legal basis:**

- Art. 6(1)(f) GDPR (our legitimate interest in improving and ensuring the stability of our services)
- Where technologies are used that require consent under applicable ePrivacy/telecom rules (e.g., accessing or storing information on end-user devices), we obtain such consent via our consent mechanism

### **Recipients:**

- Userpilot, Inc. acts as our processor. The processing does not occur on behalf of customers and is not part of the provision of the BRYTER SaaS services.

### **Data retention:**

- Personal data is stored only as long as necessary for the purposes described; aggregated or anonymized insights may be retained for longer.

## **3.10 Additional Purposes for Processing**

The data mentioned above are also processed for the additional purposes.

## **Purposes of processing:**

- To enable you to take part in events or complete surveys
- To provide, maintain, improve, and enhance our services
- To understand and analyze how you use our services and develop new products, services, features, and functionalities and deliver relevant website content or measure the effectiveness of our advertising activities
- To find and prevent fraud, and respond to trust and safety issues that may arise; and
- For compliance purposes, including enforcing our legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency
- Procurement of goods and services

## **Legal basis:**

- Art. 6 (1)(f) GDPR (legitimate interest)

## **4. Categories of recipients**

Your personal data will be disclosed to the following parties:

### **4.1 Internal recipients**

We may share your personal data with our affiliates, when supporting us in the processing activity. The legal basis for such transfer is BRYTER's legitimate interest as we provide services with cross-country teams, to guarantee smooth operations. When personal data is leaving the European Union, necessary contractual safeguards have been put in place.

### **4.2 External recipients**

We may engage third parties. These may be:

- companies and individuals (e.g. freelancer, consultants) who assist us in providing our services (e.g. payment, credit control, sanctions checks, marketing services, ICT services).
- those receiving personal data as required by law (for example if required by a court order). and under similar circumstances.
- companies' personal data is shared in connection with a merger, sale, or other asset transfer. Thereto we may transfer your information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a

corporate transaction in which we are acquired by or merged with another company, or we sell, liquidate, or transfer all or a portion of our assets. The use of your information following any of these events will be governed by the provisions of this privacy policy in effect at the time the applicable information was collected; and third parties to whom you have consented to the disclosure of personal data.

## **5. Transfers of personal data to third countries**

Your personal data will be e. g. shared with third parties and partly their sub-processors based also outside of the European Economic Area.

Third parties will only use your personal data to the extent necessary to perform their functions and are contractually bound to adhere to an appropriate level of personal data protection.

Those to be mentioned are the following:

- We use the cloud software services of Amazon Web Services (“**AWS**”) for the purpose of being able to offer our service – also BRYTER Academy and BRYTER Open. For more information, please see AWS’ privacy policy ([https://aws.amazon.com/privacy/?nc1=h\\_ls](https://aws.amazon.com/privacy/?nc1=h_ls)). We use AWS-servers that are based in the EU. AWS is based in the USA and legal basis for the transfer to AWS are the new EU Commission’s Standard Contractual Clauses.
- Asana, Inc.;
- Datadog, Inc.;
- DocSend, Inc.;
- DocuSign, Inc.;
- Glyphic AI Limited;
- Google LLC; (Analytics & Ads, incl. Google Signals and Enhanced Conversions/Customer Match): Data may be transferred to the United States for the purpose of usage analytics, cross-device reporting, audience insights and advertising measurement. Transfers rely on the EU-U.S. Data Privacy Framework where applicable and, additionally, on the European Commission’s Standard Contractual Clauses.
- Heap Inc.;
- Highspot, Inc.;
- Hubspot, Inc.;
- LearnWorlds Ltd.;

# **BRYTER**

- LinkedIn Inc.;
- We use the cloud software services of Microsoft Azure (“**Azure**”) for the purpose of being able to offer our service – also BRYTER Academy and BRYTER Open. For more information, please see Azure’s privacy policy (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1>). We use Azure-servers that are based in the EU. Azure is based in the USA and legal basis for the transfer to Azure are the new EU Commission’s Standard Contractual Clauses.
- Mixpanel, Inc.;
- Notion Labs Inc.;
- Slack Technologies, Inc.;
- Stripe Technology Company Limited (STC);
- Twitter, Inc.;
- Userpilot, Inc.
- Zendesk, Inc.;
- ZenLeads, Inc.;
- Zoom Video Communications, Inc.

Additionally, when using BRYTER Assist, BRYTER Extract and AI Connector, BRYTER engages Microsoft Corporation as a sub-processor to process Personal Data provided by Customer or End Users in order to enable the AI Services. For customers of BRYTER US, Inc. the sub-processing takes place in the European Union, the United Kingdom or the United States. For customers of BRYTER GmbH the sub-processing takes place in the European Union or the United Kingdom, unless agreed otherwise between BRYTER and Customer.

The agreements with our sub-processor specify who fulfills which data protection obligations, regarding ensuring an appropriate level of security and the implementation of your data subjects’ rights. We will be pleased to provide you with the essential content of the agreements. Please do not hesitate to contact us using the contact details given above.

## **6. Cookies and Local Storage**

### **6.1. Cookies**

We use cookies to provide you with a pleasant and secure online experience on our website.

We distinguish between the following types of cookies:

- **Technically necessary cookies:** These are required for the basic functionality and security of our website. The legal basis for their use is Art. 6(1)(f) GDPR (legitimate interest).
- **Analytics cookies:** In addition to technically necessary cookies, we use analytics cookies provided by third parties such as Google Analytics to analyze user behavior and improve our website. These analytics cookies are only set with your explicit consent via our cookie banner, in accordance with Art. 6(1)(a) GDPR (consent). You can withdraw or modify your consent at any time by accessing the cookie banner or adjusting your browser settings.

For more information about the specific cookies used, their purposes, retention periods, and how you can manage or delete them, please refer [here](#).

In addition, you can delete individual cookies or the entire cookie stock via your browser settings. Information and instructions on how to delete these cookies or block their storage in advance can be found, depending on the provider of your browser, under the following links:

- [Mozilla Firefox](#)
- [Microsoft Edge](#)
- [Google Chrome](#)
- [Opera](#)
- [Safari](#)

Please note that if you do not allow technically required or certain functional cookies, some features of our website may not be available or may function only to a limited extent.

We also implement Google Consent Mode v2, which ensures that Google services receive information about your consent status. If you do not consent, Google only receives limited cookieless pings without setting or reading cookies; if you consent, full functionality is enabled. You can change your choice at any time via “Cookie Settings”.

## 6.2. Local Storage

To enable you to customize the usage of BRYTER’s website and software to your personal needs and usage, we also use local storage technology (also known as

# BRYTER

“local data” and “local storage”) in addition to cookies. This involves storing data locally in your browser's cache, which continues to exist and can be read even after closing the browser window or exiting the program - unless you delete the cache.

Local Storage enables your preferences when using the BRYTER website and/or BRYTER's software to be stored on your computer and used by you. The following information is stored by BRYTER when using BRYTER's software as local data:

- Configuration of data views including filters, columns visible and sorting.

Third parties cannot access the data stored in local storage. It will not be passed on to third parties and will not be used for advertising purposes.

Insofar as this storage or access is absolutely necessary for us to provide the service of our website expressly requested by our website visitors (e.g., to carry out a chatbot used by the website visitor or to ensure the IT security of our website) it is carried out on the basis of Section 25 para. 2 no. 2 of the German Telecommunications Telemedia Data Protection (Telekommunikation-Telemedien-Datenschutz-Gesetz, “TTDSG”). Otherwise, this storage or access takes place on the basis of the website visitor's consent (Section 25 para. 1 TTDSG).

The subsequent data processing is carried out in accordance with the following sections and on the basis of the provisions of the GDPR.

## 7. Integration of further services

Name of the service	Service provider	Description of the service	Legal basis	Link to the privacy policy of the provider
Vimeo	Vimeo, Inc, 555 West 18th Street New York, New York 10011, USA	Integration of video content on the website	Art. 6(1)(f) GDPR	<a href="https://vimeo.com/privacy">https://vimeo.com/privacy</a>
YouTube	Google Ireland Limited,	Integration of video content on the website	Art. 6(1)(f) GDPR	<a href="https://policies.google.com/privacy?hl=de">https://policies.google.com/privacy?hl=de</a>

# BRYTER

	Gordon House Barrow Street Dublin 4, D04E5W 5, Ireland			
Google Analytics	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Web analytics for statistical evaluation and improvement of our website	Art. 6(1)(a) GDPR	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>
Google Signals (extension of Google Analytics)	Google Ireland Ltd. / Google LLC	Cross-device reporting and audience insights based on aggregated Google account information (e.g., location history, YouTube history)	Art. 6(1)(a) GDPR; Sec. 25(1) TTDSG (consent)	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>
Google Ads – Enhanced Conversions / Customer Match (User-provided Data)	Google Ireland Ltd. / Google LLC	Use of hashed customer data (e.g., email, phone) to improve conversion measurement and advertising audiences	Art. 6(1)(a) GDPR; Sec. 25(1) TTDSG (consent)	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>

Google Signals is only activated after you have given your consent in our cookie banner. You can withdraw consent at any time via “Cookie Settings” in the footer. Signed-in Google users can additionally manage ad personalisation in their own Google account at Google My Activity (<https://myactivity.google.com/>).

User-provided data for Google Ads will only be used after your explicit consent under the “Marketing” category in our cookie banner. You can withdraw consent at any time via “Cookie Settings” in the footer.

## **8. Data retention**

Your personal data will be retained as long as necessary to fulfil the legitimate purpose(s) for the processing and as long as required by law.

For Google Analytics (GA4), event-level data is retained for up to 14 months (default setting) unless you select a shorter period in the cookie banner. Aggregated analytics reports that do not allow direct identification may persist longer.

## **9. Rights of data subjects**

You have the right:

- to demand information in accordance with Art. 15 GDPR regarding the processing of your personal data by us. In particular, you may request information on the purposes of the processing, the categories of personal data, the categories of recipients to whom your data have been or are disclosed, the envisaged storage period, the existence of the right to rectification, erasure, restriction of processing or objection, the right to lodge a complaint, the source of your data to the extent that these were not collected at our site, and the existence of automated decision-making, including profiling and any meaningful information on its details;
- in accordance with Art. 16 GDPR, obtain the rectification of any inaccurate personal data stored by us or completion of such data without undue delay;
- in accordance with Art. 17 GDPR, obtain the erasure of your personal data stored by us, to the extent that processing is not required for exercising the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest or for the establishment, exercise or defence of legal claims;
- in accordance with Art. 18 GDPR, obtain the restriction of processing of your personal data, to the extent that the accuracy of the data is contested by you, processing is unlawful, but you oppose erasure and we no longer need

the personal data, but you still require them for the establishment, exercise or defence of legal claims or you have objected to processing pursuant to Art. 21 GDPR;

- in accordance with Art. 20 GDPR, demand to receive your personal data that you have provided to us in a structured, commonly used and machine-readable format or to demand transmission to another controller;
- in accordance with Art. 7(3) GDPR, to withdraw your consent once given to us towards us at any time. This has the consequence that we may no longer continue the data processing activities that were based on this consent in future and
- in accordance with Art. 77 GDPR, lodge a complaint with a supervisory authority. Usually, you may contact the supervisory authority at your habitual residence or place of work or our registered office for this.

## **10. Right to object**

As far as your personal data are processed based on legitimate interests in accordance with Art. 6(1)(f) GDPR, you have the right to object to the processing of your personal data in accordance with Art. 21 GDPR, to the extent that there are grounds relating to your particular situation or the objection is targeted against direct marketing. In the latter case, you have a general right to object that will be implemented by us without any indication of a particular situation.

If you want to exercise your withdrawal right or right to object, simply send us an email to [privacy@bryter.io](mailto:privacy@bryter.io).

## **11. How to exercise your rights**

You can also exercise the rights listed above at any time by [contacting us](#) at [privacy@bryter.io](mailto:privacy@bryter.io).

## **12. Further information**

In accordance with Art. 13(2)(e) GDPR we would like to inform you about the following:

The provision of personal data is neither a statutory nor contractual requirement, nor a requirement necessary to enter into a contract. You are not obliged to provide the personal data. There are no consequences resulting from failure to provide such data.

In accordance with Art. 13(2)(f) GDPR we would like to inform you about the following:

We do not process your personal data for the purpose of automated decision-making or to develop, improve, or train AI models or machine learning models.

### **13. Data security**

Within the website visit, we use the common SSL procedure (Secure Socket Layer) in conjunction with the respective highest encryption level your browser supports. This usually is 256-bit encryption. If your browser does not support 256-bit encryption, we will use 128-bit v3 technology instead. Whether an individual website of our internet offer is transmitted encrypted or not is evident by the closed display of the key or lock symbol in the lower status bar of your browser.

Apart from this, we use appropriate technical and organisational security measures in order to protect your data from accidental or wilful manipulation, partial or complete loss, destruction or unauthorised access by third parties. Our security measures are continuously improved in response to technological developments and the ever-changing threat landscape.

### **14. Third Parties**

Our website may contain links to other websites, products, or services that we do not own or operate. We are not responsible for the privacy practices of these third parties. Please be aware that this Privacy Policy does not apply to your activities on these third-party services or any information you disclose to these third parties. We encourage you to read their privacy policies before providing any information to them.

### **15. Children's Privacy**

We do not knowingly collect, maintain, or use personal information from children under 13 years of age, and no part of our website is directed to children. If you learn that a child has provided us with personal information in violation of this Privacy Policy, then you may alert us at [privacy@bryter.io](mailto:privacy@bryter.io).

### **16. Topicality and changes of this data privacy statement**

This privacy policy is currently valid as of January 2026.

Further development of our website and offers through it or changed statutory or authority specifications may require changes to this privacy policy. You may call and print the respective current data privacy statement at any time on the website. If we materially change the ways in which we use or share personal data previously

**BRYTER**

collected from you, we will notify you through the website, by email, or other means of communication.