DATA PROCESSING AGREEMENT

Effective Date: 27 March 2026
Last Updated: 27 March 2026

Parties

Between

Customer (the "Controller") - as specified in the Main Agreement

and

beCrystal AS, a company registered in Norway with organization number 933660192, having its registered office at Gaustadalléen 21, 0349 Oslo, Norway (the "**Processor**")

an agreement on the processing of personal data is entered into (the "**Agreement**") on the background of an agreement entered into where the Processor is the supplier, and the Controller is the customer (the "**Main Agreement**"). The Agreement forms an integral part of the Main Agreement.

1. Background and purpose of the processing

The Processor shall process the personal data on behalf of the Controller concerning the above-said.

The subject and purpose of the processing of personal data, the duration of the processing of personal data, the subject matter of the processing of personal data, the types of personal data to be processed, the categories of data subjects to whom the personal data relates and other obligations and rights of the Controller are included in Appendix to this Agreement.

This Agreement shall provide for the processing of personal data in accordance with the regulation the EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**") as implemented into Norwegian legislation in the Personal Data Act (LOV-2018-06-15-38), and in accordance with other relevant legislation which

concerns the processing of personal data under the Agreement ("**Personal Data Regulation**").

The Processor shall process the personal data only on documented instructions as described in the Agreement.

Terms and definitions used in the Agreement shall be construed in the same way as in the Personal Data Regulation.

2. The Processor's duties

The Processor confirms that it will implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the Personal Data Regulation and ensure the protection of the rights of the data subject, inclusive comply with the requirements in GDPR Article 32. Other duties are set forth under Section 5.

The Processor shall, considering the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in GDPR Chapter III. The Processor may claim compensation for time spent, and reasonable and necessary expenses incurred as a result of such assistance. In addition, the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of processing and the information available to the Processor.The Processor may claim compensation for time spent, and reasonable and necessary expenses incurred as a result of such assistance.

The Processor shall make available to the Controller all information required under applicable law to demonstrate compliance with the obligations laid down in this Section 2. To the extent the Controller's audit requirements under GDPR cannot reasonably be satisfied through audit reports, documentation, or other compliance information that the Processor makes generally available to its customers, Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, which is reasonable and necessary under the legal obligations.

The Processor has a duty of confidentiality regarding the personal data and other information the Processor receives as part of the Agreement and the processing of personal data, and shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Any requests regarding the personal data or the processing from others or the data subject, or any inquiry or request for disclosure from an authority regarding personal data provided by the Controller to the Processor, shall be forwarded to the Controller without undue delay if not otherwise agreed in this Agreement or by instruction by the Controller.

If the Processor is in the opinion that an instruction by the Controller infringes the Personal Data Regulation, the Processor shall immediately inform the Controller.

3. Duties and rights of the Controller

The Controller is responsible for ensuring that personal data is processed in accordance with the Personal Data Regulation, and has both a right and an obligation to decide which purposes and which aids can be used in the processing carried out by the data processor. Therefore, the Controller must provide the data processor with documented instructions for how personal data is to be processed, where the instructions can either be part of this Agreement or attached to the Agreement.The Controller is the controller of the personal data and is responsible for the accuracy, integrity and reliability of the data and is responsible for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

4. Use of subcontractor/sub-processor

The Controller acknowledges and consents to beCrystal's utilization of sub-processors as listed at https://becrystal.ai/privacy/subprocessors. beCrystal reserves the right to modify this list by adding new sub-processors as needed, and will inform the Controller of such changes.

Should the Controller wish to contest the addition of a new sub-processor, they must submit a written objection to the Processor within a 30-day window following the notification. Upon receiving an objection, both parties commit to collaboratively seeking a resolution. This may involve making reasonable adjustments to the Controller's service configuration or agreement to circumvent personal data processing by the new sub-processor.

Objections can only be raised on the grounds that the new sub-processor's inclusion would result in the Controller violating their data protection obligations or other relevant legal requirements. If no objection is raised within the specified timeframe, the new sub-processor will be deemed accepted by the Controller. If beCrystal decides to proceed with the change despite the Controller’s reasonable objections,

the Controller has the right to terminate the Main Agreement for convenience within 30 days of the change being implemented.

Any sub-processor shall be imposed the same obligations as the Processor set forth in the Agreement in a written, binding agreement wherein the sub-processor is providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Personal Data Regulation. Where that sub-processor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for performing the subprocessor's obligations.

5. Security of processing and notification of breach

The Processor shall comply with the requirements for security given in the Personal Data Regulation and such best practice/branch standards the Processor deems relevant for the processing. The Processor shall provide documentation of technical and organizational measures implemented to ensure the security of the personal data upon the request of the Controller.

In case of a personal data breach, the Processor shall without undue delay notify the Controller. Such notification shall at least:

1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. communicate the name and contact details of the contact point where more information can be obtained;
3. describe the likely consequences of the personal data breach;
4. describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If not all information above may be given in the first notice, the information shall be provided as soon as possible.

The Controller is responsible for notifying the supervisory authorities, such as Datatilsynet in Norway, and the Processor is not to contact or notify the supervisory

authorities without the explicit instruction by the Controller, if such information reveals the name of the Controller.

6. Transfer to countries outside the EEA (third countries)

Personal data shall only be transferred to third countries, i.e. countries outside EU/EEA or to countries other than those considered by the European Commission to have an adequate level of protection, if the conditions laid down in the provisions of GDPR relating to the transfer of personal data to third countries or international organisations are met by the Processor.

For the transfer to or access from third countries for personal data, it is required that the appropriate safeguards, including with regard to the rights of data subjects, be complied with. The Processor can ensure compliance with such conditions by using standard contractual clauses, provided the conditions for the use of those standard contractual clauses are met.

7. Term. Instruction to stop the processing. Effect on termination

This Agreement shall be effective and stay in force as long as the Processor (and its permitted sub-processors) processes personal data on behalf of the Controller in the context of the Main Agreement.

Upon breach of this Agreement, of instructions given by the Controller or on the Personal Data Regulation, the Controller may instruct the Processor to stop the processing of the personal data with immediate effect.

Upon termination of this Agreement, regardless of reason, the Processor (and its permitted sub-processors) shall within 60 days delete or return any or all personal data to the Controller, subject to the Controllers instructions, in a standardized format and medium along with necessary instructions to facilitate the Controller's further use of such data, and delete all copies of those personal data.

The Controller shall upon request receive a written confirmation from the Processor that all personal data has been returned or deleted according to the Controller's instructions.

8. Other duties and rights

Other obligations and rights are governed by the Main Agreement between the Controller and the Processor regarding the services that necessitate the processing of personal data and this Agreement.

If the Main Agreement is transferred, this Agreement shall be transferred accordingly.

Appendix A – Details on Processing

For the Controller, contact information is to be provided by the Controller through an online purchase system or specified in relevant order documents such as the Main Agreement.

beCrystal AS serves as the Processor. beCrystal's contact details are Gaustadalléen 21, 0349 Oslo, Norway and email dpo@becrystal.ai.

Data subjects whose Personal Data are transferred

- The Controller's business contacts, including prospective and current customers, partners, and individual vendors.
- People working on behalf of the Controller, such as staff members, representatives, advisors, and freelance professionals.
- End-users of the Controller
- Any natural person who becomes identifiable through information provided by the Controller while using the service.

Types of Personal Data Involved in Transfers

The Agreement covers various categories of personal data that may be processed:

- Identity and access details, including individual names, chosen usernames, email addresses, and security credentials.
- Public-facing profile data, which might encompass names, visual representations like avatars or photographs, workplace information, professional titles, postal addresses, links to social media profiles, and personal or professional biographies.
- Contact details necessary for communication, such as names, physical addresses, email addresses, and phone numbers.
- Information shared during customer support interactions, detailing service requests and assistance provided.
- Usage analytics data that allows the Controller to assess engagement levels of their authorized users, including metrics and statistical information related to service utilization.

Sensitive categories of Personal Data

beCrystal maintains a policy against deliberately collecting or processing sensitive or special categories of Personal Data. This includes, but is not limited to, genetic information, health-related data, or details about religious affiliations.

The Controller is advised not to submit such sensitive data to the Processor's services without prior explicit agreement, as outlined in the relevant section of the Subscription Agreement.

However, in the event that the Controller does transmit sensitive or special categories of Personal Data to the Processor's services without obtaining prior consent, such information will still be protected. In these instances, the data will fall under the scope of the technical and organizational security measures that the Processor has implemented, as detailed in the security appendix to this agreement.

The nature and purpose of processing

The processing activities are directly tied to the Controller's utilization of the Processor's services. The specific purposes and parameters of this processing are determined and managed exclusively by the Controller, according to their own requirements and objectives.

The primary reason for transferring data is to enable beCrystal to deliver its services effectively.

Use of a Secure Pre-Production Environment for Continuous Service Delivery

To ensure the quality, security, and accuracy of the service on an ongoing basis, the Processor will process Controller Personal Data in a secure, logically-isolated pre-production environment. The purpose of this processing is to prepare, validate, maintain, and improve data and configurations for the production system. This is a necessary step for the continuous performance of the contracted services throughout the term of the Agreement.

This pre-production environment is subject to technical and organizational security measures that are identical to those of the production environment as described in this Agreement. Access to Controller Personal Data within this environment is strictly limited to authorized personnel on a need-to-know, tenant-specific basis. Data will be retained in this environment for the duration of the Agreement and will be permanently deleted from this environment within sixty (60) days following the

termination of the Master Agreement. This processing is included within the scope of this Agreement.

Retention

Generally, the Processor will maintain the Personal Data for the duration of the Controller's active subscription. Once the subscription term concludes, the data retention period typically ends, unless otherwise specified by the Controller.

However, there are two key exceptions to this general rule:

- Certain laws or regulations may necessitate the retention of specific data beyond the subscription term.
- The Master Agreement between the Controller and Processor may include clauses that allow for extended data retention under particular circumstances.

These exceptions ensure compliance with legal obligations and agreed-upon terms, while still prioritizing the Controller's authority over their data. The Processor will adhere to these retention guidelines, balancing the Controller's preferences with any applicable legal or contractual requirements.

Appendix B – Security Measures in the Processing

beCrystal commits to implementing and maintaining a comprehensive set of security measures to protect Personal Data. These measures are designed to ensure the confidentiality, integrity, and availability of data processed on behalf of the Controller.

The security framework includes technical and organizational safeguards specifically tailored for beCrystal's services. These measures are documented and regularly updated to address evolving security challenges and best practices in data protection, found at https://becrystal.ai/security.

beCrystal operationalizes security through a set of policies and continuous training.

Extending this security commitment, beCrystal requires its sub-processors to implement and maintain security measures that are substantially equivalent to its own standards. This approach ensures a consistent level of protection throughout the data processing ecosystem.