

Agreement for Order Data Processing Brandic 365

Supplementary Terms and Conditions for Order Data Processing

within the meaning of Art. 28 (3) of the EU General Data Protection Regulation (“GDPR”) (hereinafter: “**the ODP Agreement**”) between Brandic Software GmbH, Bahnhofstrasse 6, CH-6340 Baar ZG, Switzerland (hereinafter: “**the Provider**”) and its customer (hereinafter: “**the Contractor**”) (hereinafter jointly referred to as: “**the Parties**”).

In order to regulate the terms and conditions of certain data processing operations provided by the Provider to the Contractor as part of the contractual provision of services by the Provider within the meaning of Art. 28 GDPR in accordance with applicable data protection law, the Parties enter into the following ODP Agreement:

1. Scope of application, subject and duration of the ODP Agreement

- 1.1. **Subject of the ODP Agreement:** The ODP Agreement sets out the rights and obligations of the Parties under data protection law arising from the Client’s option, as agreed between the Parties, to use software, applications or functions (such as service packages) (hereinafter collectively referred to as: “**Software**”) via the Internet (as Software-as-a-Service (“SaaS”), cloud services or other data processing services) in accordance with the respective applicable General Terms and Conditions of the Provider and any other documents of the Provider governing the provision of services (hereinafter: “**the Main Agreement**”). In this context, it shall apply to all activities in which employees of the Provider or third parties commissioned by the Provider process personal data within the meaning of Art. 4 No. 1 GDPR (hereinafter: “**Data**”) of the Client pursuant to Art. 28 GDPR. Insofar as the term “data processing” or “processing” (of data) is used in this ODP Agreement, the definition of “**processing**” within the meaning of Art. 4 No. 2 GDPR shall apply.
- 1.2. **Duration and termination of the Agreement:** This ODP Agreement shall enter into force upon conclusion of the Main Agreement and shall apply for the duration thereof. Insofar as personal data of the Contractor is actually processed by the Provider beyond the term of the ODP Agreement (e.g. in the case of storage of data due to statutory retention obligations to which the Provider is subject), the contractual agreements on purpose limitation and compliance with the technical and organisational measures shall continue to apply.
- 1.3. **Details of data processing:** The type of data, the nature and purpose of data processing as well as the categories of data subjects are specified in the Main Agreement and the associated service description as well as in Annex B.

2. Responsibility

- 2.1. **Permissibility of data processing:** The Contractor is aware that, within the framework of the Main Agreement, it alone bears the sole responsibility as the responsible party ("**Controller**" within the meaning of Art. 4 No. 7 GDPR) for compliance with the statutory provisions of the data protection laws, in particular the responsibility for the lawfulness of the transfer of data to the Provider, as well as the lawfulness of the data processing, and shall create the conditions within its area of responsibility to ensure that the Provider can provide the agreed services without infringing the law.
- 2.2. **Instructions:** The Contractor shall have the right to issue instructions under the Main Agreement. The instructions are defined by the Main Agreement and can be changed, supplemented or replaced by the Contractor in written form by individual instructions ("**individual instructions**"). Verbal instructions must be confirmed by the Contractor without delay at least in text form (e-mail is sufficient). Instructions which are not provided for in the Main Agreement shall be treated as a request for a change to the services to be remunerated separately. The Parties shall mutually agree on an appropriate remuneration. Insofar as arrangements on changes to the services have been agreed in the Main Agreement, these shall take precedence over the provisions of this subsection 2.2.

3. Obligations of the Provider

- 3.1. **Data processing:** The Provider may only process data within the scope of the purpose stated in the Main Agreement and in accordance with the Client's instructions, unless an exceptional case exists in accordance with Art. 28 (3) (a) GDPR. If the Provider is of the opinion, based on its industry or specialist knowledge, that an instruction of the Contractor violates applicable data protection regulations, it shall notify the Contractor thereof without undue delay. The Provider shall be entitled to suspend the implementation of the relevant instruction until it is confirmed in writing by the Client or amended. If the Provider is of the opinion that processing in accordance with the instructions may lead to liability on the part of the Provider (e.g. in accordance with Art. 82 GDPR), it shall be entitled to suspend further processing until the liability between the Parties has been clarified. However, the provider is not obliged to carry out a substantive review of the lawfulness of instructions.
- 3.2. **Support for obligations of the Controller:** The Provider shall, taking into account the nature of the processing and the information available to it, provide the Contractor with appropriate support upon request to the extent necessary and within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III GDPR and in complying with the **Contractor's obligations as set out in Art. 32 to 36 GDPR**. The Provider shall be entitled to charge the Contractor for the expenses incurred in this regard on the basis of the Provider's hourly rate applicable at the time, unless the Parties agree otherwise.

- 3.3. **Reliability of the employees:** The employees and other persons working for the Provider who are involved in the processing of the Contractor's data shall be familiarised by the Provider with the data protection regulations applicable to them and shall be bound to secrecy in an appropriate manner. In this context, the Provider's employees are prohibited from processing the Contractor's data outside the scope of the instruction and must treat the Contractor's data confidentially. This confidentiality obligation shall continue to exist after completion of the order.
- 3.4. **Contact person of the Provider:** Upon request, the Provider shall name a contact person for the Contractor for data protection issues arising within the scope of this ODP Agreement. The Provider shall inform the Contractor without undue delay of any change of contact person.
- 3.5. **Procedure in the case of data breaches:** The Provider shall inform the Contractor without undue delay if it becomes aware of breaches of the Contractor's personal data. The Provider shall take the necessary measures to secure the data and to mitigate possible adverse consequences for the data subjects and for this purpose shall consult with the Contractor without delay.

4. Obligations of the Contractor

- 4.1. **Support by the Contractor:** The Contractor shall inform the Provider without delay and in full if it finds errors or irregularities regarding data protection regulations in the order results.
- 4.2. **Contact person of the Contractor:** Upon request, the Contractor shall name a sufficiently authorised contact person for the Provider for all data protection issues arising within the scope of the ODP Agreement. The Contractor shall inform the Provider without undue delay of any change of contact person.

5. Technical and organisational measures for data security (Art. 32 GDPR)

- 5.1. **Technical / organisational measures:** The Provider shall arrange its internal organisation in such a way that it meets the requirements of data protection to the necessary extent. To this end, the Provider shall take technical and organisational measures to adequately protect the data processed on behalf of the Contractor which meet the requirements of Art. 32 GDPR. The technical and organisational measures taken by the Provider at the time of the conclusion of this ODP Agreement are attached in **Annex A**. The Contractor has assessed these measures against the background of the specifically agreed data processing operations with regard to an appropriate level of protection and found them to be sufficient.
- 5.2. **Adjustments:** The Provider may change the measures taken at any time, provided that it is ensured that the agreed level of protection is not undercut. The Provider shall inform the Contractor of any significant changes to its technical and organisational measures.

6. Correction, deletion and blocking of data

- 6.1. **Support for correction, deletion, blocking:** The Provider shall correct, delete or block the data processed on behalf of the Contractor at any time in accordance with the Contractor's instructions, provided that this does not conflict with the Provider's legitimate interests. The Provider shall be entitled to charge the Contractor for the expenses incurred in this regard on the basis of the Provider's hourly rate applicable at the time, unless the Parties agree otherwise.
- 6.2. **Completion of contract work, return or deletion:** For the termination of the order, the Contractor instructs the Provider to delete the Contractor's data still held by the Provider. The Contractor is entitled to issue deviating instructions for the deletion or surrender of its data in the event of termination of the order. However, the Provider shall be entitled to invoice the expenses incurred in the event of deviating instructions by the Contractor on the basis of the Provider's hourly rate applicable at the time, unless the Parties agree otherwise.
- 6.3. **Storage by the Provider:** If legitimate interests of the provider (e.g. statutory retention periods) prevent deletion, the data will only be deleted after the interest has ceased to exist.

7. Establishment of subcontracting relationships

- 7.1. **Authority to subcontract:** The Provider is permitted at any time to establish subcontracting relationships with affiliated companies or third parties (i.e. with service providers who support the Provider in the provision of services and thereby obtain access to the Contractor's data, e.g. data centres) in accordance with this subsection 7. At the time of the conclusion of this Agreement, the companies listed in **Annex B** are active as sub-processors for the Provider within the scope of the partial services provided and directly process the Contractor's data. For these subcontractors, the Contractor's consent shall be deemed granted upon conclusion of the ODP Agreement.
- 7.2. **General written consent:** If the Provider commissions further processors within the meaning of Art. 28 (4) GDPR (hereinafter referred to as "**sub-processors**"), the Contractor shall, however, be informed so that it can prohibit the commissioning by objecting if there are important reasons. If the Contractor does not object within 4 weeks after being informed by the Provider, the Contractor's consent shall be deemed given. The Provider shall make arrangements with its sub-processors for order data processing which at least meet the requirements of these Terms and Conditions.
- 7.3. **Excluded subcontractors:** Subcontracting relationships not subject to the obligation to provide information within the meaning of subsection 7.1 are those services which the Provider uses from third parties as a purely ancillary services in order to carry out its commercial activities and which are not specifically geared to the processing of personal data. This includes, for example, cleaning services, pure telecommunication services without any specific reference to services which the Provider renders for the Contractor, postal and courier services, transport services, security services. Nevertheless, in the case

of ancillary services provided by third parties, the Provider is also obliged to ensure that appropriate precautions and technical and organisational measures have been taken to ensure the protection of personal data.

- 7.4. **Exception to the duty to inform:** In the event of important reasons under data protection law or compelling technical reasons on the part of the Provider which require the immediate use of an additional sub-processor (in particular in emergency situations, for reasons of data security, to maintain the contractually agreed activity or to avert imminent damage or to avoid the intensification or extension of damage which has already occurred), the sub-processor may be engaged immediately, in derogation of subsection 7.1.
- 7.5. **Territorial scope of application/authorisation:** The Provider is entitled to transfer personal data of the Contractor to subcontractors in a third country and to have them process such data, provided that the mandatory statutory provisions for data exports to third countries are met.

Insofar as EU Standard Contractual Clauses are used for this purpose, the Provider shall, if necessary, conclude these in the name of and on behalf of the Contractor or shall authorise its subcontractor to conclude the EU Standard Contractual Clauses in the name of and on behalf of the Contractor with its sub-subcontractor. **The Contractor hereby grants the necessary power of attorney.** In the event of a conflict between mandatory provisions of the EU Standard Contractual Clauses (if entered into on a supplementary basis) and this ODP Agreement and the accompanying Annexes, the provisions of the Standard Contractual Clauses shall prevail. In the event of all other conflicts between the Main Agreement, this ODP Agreement shall prevail for issues relating to data protection law.

The Provider shall provide the Contractor with the necessary data and information to prove compliance with the statutory provisions for data exports to third countries in advance upon request. Processing operations or transfers to a third country existing at the time of the conclusion of this ODP Agreement are set out in **Annex B**.

- 7.6. **Sub-subcontractors:** The use of sub-subcontractors is governed by this subsection 7.

8. Verification possibilities & control rights

- 8.1. **Verifications, burden of proof on the supplier:** The Contractor may, at its own expense, monitor the Provider's compliance with the data protection provisions and obligations of this ODP Agreement by obtaining information or evidence with regard to the data processing operations concerned. The Provider shall, at the Contractor's request and within a reasonable period, provide the Contractor with evidence of compliance with its obligations under this ODP Agreement by appropriate means of its choice (e.g. by conducting a self-audit, submitting a current audit certificate or a self-disclosure, reports or report extracts from independent bodies such as accountants, auditors, data protection officers, IT security department, data protection auditors, quality auditors) certificates on data protection and/or information security (e.g. in accordance with BSI

basic protection requirements or ISO 27001) or certificates in accordance with Art. 42 GDPR.

- 8.2. **Inspections:** The Contractor shall primarily check whether the inspection options granted in subsection 8.1. are sufficient. Moreover, if, in justified exceptional cases (for example, in the event of justified doubts that evidence within the meaning of 8.1 is insufficient or inaccurate, or is not provided, or in the event of special incidents pursuant to Art. 33 (1) GDPR), inspections by the Contractor or by an auditor commissioned by the Contractor at its own expense are necessary in individual cases to ensure compliance with the obligations of this ODP Agreement, in particular the technical and organisational measures taken, such inspections shall be carried out during the Provider's normal business hours without disrupting its operations following prior notification. The Provider may make control measures of the Contractor dependent on prior written notification with an appropriate lead time (at least 14 days) and naming at least three alternative dates as well as on the signing of a confidentiality agreement with regard to the data of other customers and the technical and organisational measures implemented, unless special incidents justify a control deviating from this. If the inspector commissioned by the Contractor is a competitor of the Provider, the Provider shall have the right to object to them. On-site inspections by the Contractor shall, except in the case of important data protection reasons, generally be organised as spot checks of the areas relevant for the performance of the order data processing and shall be limited to a maximum of one day per calendar year.
- 8.3. **Compensation for inspection expenses:** Insofar as an inspection was not necessary due to misconduct on the part of the Provider and insofar as no significant deviations from the Provider's obligations under this ODP Agreement were identified, the Provider shall be entitled to invoice the Contractor for the expenses incurred for inspection measures pursuant to Section 8.2 on the basis of the Provider's hourly rate applicable at the time, unless otherwise agreed between the Parties. This also applies to inspections or controls by the Contractor, by a data protection supervisory authority or any other sovereign supervisory authority.

9. Requests by data subjects

- 9.1. **Notification of requests:** If a data subject should contact the Provider directly to request the correction, deletion of their data or information, the Provider shall refer the data subject to the Contractor, provided that an allocation to the Contractor is possible based on the information provided by the data subject. The Provider shall forward the data subject's request to the Contractor without delay.
- 9.2. **Assistance with data subject rights:** The Provider shall support the Contractor at the Contractor's instruction with information required by the Contractor to respond to requests by the data subject. The Provider shall be entitled to charge the Contractor for the expenses incurred in this regard on the basis of the Provider's hourly rate applicable at the time, unless the Parties agree otherwise.

- 9.3. **Responsibility for data subject rights:** The Provider shall not be liable if the Contractor fails to respond to the data subject's request or does not do so correctly or in a timely manner.

10. Third-party measures or third-party rights with regard to data

If items containing data are affected by third-party measures (such as seizures or confiscations) or by third-party rights (transfer of ownership by way of security), the Provider shall inform the Contractor without delay. The Provider shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Contractor as the "Controller" within the meaning of the General Data Protection Regulation.

11. Liability

- 11.1. **Liability:** The liability provisions agreed between the Parties in the Main Agreement shall also apply to the present order data processing, unless expressly agreed otherwise.
- 11.2. **Mutual support:** In the event of a claim being made against one of the Parties by a data subject with regard to any claims under Art. 82 GDPR or a supervisory authority on the basis of or in connection with this ODP Agreement, the respective other party undertakes to provide the party against which a claim is made with appropriate support in defending against the claims.
- 11.3. **Contractor's area of responsibility, indemnity:** Insofar as damage is caused by inadmissible or incorrect data processing within the scope of this Order Data Processing Agreement and this damage was caused by the correct implementation of the commissioned services or an instruction issued by the Contractor, the Contractor alone shall be liable for this. The Contractor shall indemnify the Provider against all claims made by third parties against the Provider in connection with the specific implementation of the commissioned service or the instruction issued by the Contractor. Under these conditions, the Contractor shall also reimburse the Provider for all legal defence costs incurred.

12. Final provisions

- 12.1. **Amendment of the ODP Agreement** Amendments and supplements to this ODP Agreement and all of its components - including any assurances by the Provider - shall require a written agreement, which may also be in an electronic format ("**text form**"), and an express indication that it is an amendment or supplement to these conditions. This also applies to any waiver of this formal requirement.
- 12.2. **Validity of the ODP Agreement:** Should individual provisions of this ODP Agreement be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions. In the event of the invalidity of a clause, the Parties shall agree on a substitute provision based on the economic purpose of the agreement. The same shall apply mutatis mutandis to incomplete provisions.

- 12.3. **Place of jurisdiction, applicable law:** This ODP Agreement shall be governed exclusively by German law including the provisions of the GDPR to the exclusion of the provisions of the UN Convention on Contracts for the International Sale of Goods (CISG). International private law shall not apply. The exclusive place of jurisdiction for all disputes arising from or in connection with this ODP Agreement is the Provider's place of business. The choice of venue is exclusive only for the Contractor.
- 12.4. **Terms and Conditions:** The Contractor's general terms and conditions of business or purchase shall not apply to this ODP Agreement. This ODP Agreement shall apply exclusively vis-à-vis the Contractor even if the Provider performs its services without reservation even in the knowledge of conflicting general terms and conditions of business or purchase.
- 12.5. **Order of priority:** In the event of contradictions between the contents of this ODP Agreement and the provisions of the Main Agreement with regard to data protection issues, this ODP Agreement shall prevail. In all other respects, the provisions of the Main Agreement shall remain unaffected and shall apply accordingly to this ODP Agreement.
- 12.6. **Annexes:** The Annexes listed below shall become an integral part of this ODP Agreement:
- **Annex A:** Technical and organisational measures pursuant to Art. 32 GDPR will be made available on request
 - **Annex B:** Subcontractors, details of data processing

Annex B to the Supplementary Terms and Conditions for Order Data Processing: Subcontractors, details of data processing, details on technologies

This Annex B, in conjunction with the ODP Agreement, regulates the modalities for the order data processing in connection with the Main Agreement concluded between the Parties as a supplement to the Main Agreement.

Approved subcontracting relationships at the time of conclusion of the agreement

- At the time of the conclusion of the Agreement, no subcontractors were used to process the Contractor's data:
- Subcontracting relationships at the Provider at the time of the conclusion of this Agreement:

The following companies are associated with the contractor and provide a partial service:

| Subcontractor (company, address) | Type of partial service (processing steps / purpose of order processing) | Place of performance |
|--|--|-----------------------------|
| PrimeDocs GmbH, 80992 München | Monitoring of the systems at Microsoft, updating of the Brandic 365 software, template construction and implementation | Germany |
| ZigWare GmbH, 6340 Baar | Monitoring of the systems at Microsoft, updating of the Brandic 365 software, template construction and implementation | Switzerland |
| Sevitec Informatik AG, 8360 Eschlikon | Monitoring of the systems at Microsoft, updating of the Brandic 365 software, template construction and implementation | Switzerland |

The following companies are not associated with the contractor and provide a partial service:

| Subcontractor (company, address) | Processed data categories | Type of partial service (processing steps / purpose of subcontracting) | Place of performance |
|---|--|---|-----------------------------|
| Microsoft Azure Datacenter Netherland (Amsterdam) (Release 2020) | Personal data for use in the created documents | Application operation, data storage from the source from the customer. | Netherlands |

Description of the order data processing

1. Object of the data processing

The scope, subject, nature and purpose of the data processing

- Includes the execution of the following tasks by the contractor: Acquisition, processing and storage of employee-related data for the automatic filling of Microsoft Office templates in the software solution Brandic 365 (SaaS solution). The software solution only serves as a synchronisation receiver for personal data.

2. Type of data, categories of data subjects

The following types of data/data categories are affected by the data processing (multiple answers possible):

- Personal data (e.g. surname, first name, gender, date/place of birth, identification numbers, nationality, etc.)
- Communication data (e.g. address, e-mail address, telephone number, mobile phone number)
- Contract master data (e.g. contractual relationship, product or contractual interest, products purchased, date of purchase agreement, purchase price).

The following categories of persons are affected by the data processing (multiple answers possible):

- Other business partners (Any (natural or legal) person with whom a business relationship exists (with the respective Controller) other than customers) e.g. suppliers, importers or service partners themselves; intermediaries, shareholders, freelancers, etc.
- Employees of the Contractor
- Contact persons of the Provider attributable to the Contractor (any natural person who does not fall under the employee definition such as employees of partner companies (employees of a supplier, service provider, joint venture, temporary employment agency), group employees (employees of another group company))

3. Infrastructure and used technologies

Microsoft Azure

Brandic 365 uses Microsoft Azure functionalities and services to process and store the above-mentioned categories of data. The Microsoft Azure platform and the Microsoft data centers correspond to the latest technology, also in terms of security and data protection standards.

Further information can be found at: <https://www.microsoft.com/en/trust-center/>

Microsoft «Azure Application Insights»

Brandic 365 uses the "Application Insights" services from Microsoft Azure to monitor live applications in order to identify any anomalies in performance.