**EU-DATENSCHUTZ-GRUNDVERORDNUNG**

**MUSTERVERTRAG – englische Sprache**

Agreement

concerning

data processing by a processor in accordance
with Art. 28 GDPR

Die Experten der Wirtschaftskammern Österreichs haben für ihre Mitgliedsbetriebe nachstehendes Muster einer Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO erstellt.

Das hinterlegte Wasserzeichen „Muster“ kann einfach aus dem Word-Dokument entfernt werden.

Dieser Mustervertrag ist auf eine **Auftragsverarbeitung in Österreich zugeschnitten.** Für die Auftragsverarbeitung innerhalb der EU, des EWR oder in [Staaten mit angemessenem Datenschutzniveau](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de) werden die [Standardvertragsklauseln](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915) (Durchführungsbeschluss 2021/915) empfohlen. Bei Verarbeitungen in Drittstaaten ist die Verwendung der Standarddatenschutzklauseln (Durchführungsbeschluss 2021/914) zwingend, anderenfalls Genehmigungspflichten entstehen können.

Weitere Informationen zum internationalen Datenverkehr finden Sie hier:

[EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Internationaler-Datenverk.html).

Link zu den Standardvertragsklauseln laut Durchführungsbeschluss 2021/915 im Word-Format: [„Standard contractual clauses for controllers and processors in the EU/EEA (Word)“](https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_de) / [ZIP-Download für alle Sprachfassungen](https://commission.europa.eu/document/download/a53e88fe-3b08-4e83-8587-4e3869ebb1c3_en?filename=strandard_contractual_clauses_eu-eea.zip).

**Zum Verhältnis der Standardvertragsklauseln laut Durchführungsbeschluss 2021/915 zu diesem Muster („traditionell österreichischer Mustervertrag“) für die Auftragsverarbeitung nach Art 28 DSGVO**: Abgesehen von einer unterschiedlichen Gliederung, fehlen im traditionell österreichischen Mustervertrag klassische Vertragsklauseln, wie sie sich in den Klauseln 1 bis 4 der EK-AVV-Klauseln finden, die gesonderte Erwähnung sensibler Daten (Klausel 7.5.), die Dokumentationspflichten (Klausel 7.6.) sowie die Drittbegünstigungsklausel (Klausel 7.7. lit e), da diese nicht als essenziell gesehen werden. Die EKK-AVV-Klauseln führen ferner die Mitwirkungspflichten des Auftragsverarbeiters näher aus (vgl. Klauseln 8 und 9).

Im Gegenzug berücksichtigt der traditionell österreichische Mustervertrag rechtliche Besonderheiten wie das Format der Daten bei Rückgabe infolge Beendigung der Auftragsverarbeitervereinbarung (siehe Punkt 3.8.).

**Zum Verhältnis zu den Standarddatenschutzklauseln laut Durchführungsbeschluss 2021/914:** Diese decken alle Arten von Datentransfers in Drittländer (Staaten ohne angemessenes Datenschutzniveau) ab, nicht nur Datentransfers zwischen Verantwortlichem und Auftraggeber (siehe dazu auch Klausel 2 lit a Durchführungsbeschluss 2021/914).

Siehe dazu: [EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Internationaler-Datenverk.html)

Dieser Mustervertrag wurde mit größter Sorgfalt erstellt und kann laufend aktualisiert werden. Für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters sowie auch für weiterführende Links können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster bereitgestellt haben, sind daher ausgeschlossen.

Wir behalten uns ausdrücklich vor, das Muster ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen und übernehmen daher keine Gewähr und Haftung für die dauerhafte Verfügbarkeit der des Musters.

Stand: Juli 2023

Dies ist ein **Produkt der Zusammenarbeit aller Wirtschaftskammern**.

Bei Fragen wenden Sie sich bitte an die Wirtschaftskammer Ihres Bundeslandes:

Burgenland, Tel. Nr.: 05 90907, Kärnten, Tel. Nr.: 05 90904, Niederösterreich Tel. Nr.: (02742) 851-0,

Oberösterreich, Tel. Nr.: 05 90909, Salzburg, Tel. Nr.: (0662) 8888-0, Steiermark, Tel. Nr.: (0316) 601-0,

Tirol, Tel. Nr.: 05 90905-1111, Vorarlberg, Tel. Nr.: (05522) 305-0, Wien, Tel. Nr.: (01) 51450-1010.

**Hinweis!** Diese Information finden Sie auch im Internet unter <http://wko.at>/datenschutz. Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammern Österreichs ist ausgeschlossen.

Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter!

Agreement

concerning

data processing by a processor in accordance
with Art. 28 GDPR

|  |  |  |
| --- | --- | --- |
| The controller: |  | The processor: |
| **[*NN*]**[*Address*] |  | **[*NN*]**[*Address*] |
| (Hereinafter referred to as client]  |  | (Hereinafter referred to as contractor) |

# Subject matter of the agreement

1. The subject matter of this agreement is the implementation of the following tasks: [*a detailed description of the tasks of the contractor, including the type and purpose of the intended processing*].

{In case of a framework agreement, service agreement, performance agreement, or similar is in place} This agreement is to be considered a supplementary document to [*add contract etc including* *date*].

1. The following data categories are processed: [*list data categories, e.g. contact, contract, invoice, credit-history, order and payment details etc*].
2. The following categories of data subjects are subject to this processing [*add categories of data subjects, e.g. clients, interested parties, suppliers, points of contact, employees etc.*]

# Duration of the agreement

{Single implementation} The agreement ends with a single execution of the tasks.

{Temporary duration} The agreement is temporary and ends with [*add deadline*].

{Unlimited duration} The agreement does not have a defined endpoint and can be ended by either party with a notice period of [*add notice period e.g. one month*] on [*add notice date e.g. every quarter*]. The option to terminate due to exceptional circumstances remains unaffected.

# Obligations of the contractor

1. The contractor commits himself to process the data and the processing results exclusively within the scope of the written assignment of the client. Should the contractor be required to release data of the client by request of the authorities, then he has to – as far as it is legally permitted - inform the client of the above without delay and refer the authorities to the client. Likewise, the processing of data for the contractor’s own benefit requires written approval by the client.
2. The contractor declares legally binding that he has obligated all persons, assigned to process the data, to adhere to the confidentiality practices, prior to the beginning of the task, or that they are bound by an appropriate, legal non-disclosure obligation. The non-disclosure obligations are upheld, even when their assignment is completed and the contractor no longer employs them.
3. The contractor declares that he has taken all required steps to ensure that the security of the processing is upheld in accordance with Art. 32 GDPR (for specifications see appendix ./1).
4. The contractor implements the appropriate technical and organisational measures so that the client can comply with the rights of the affected individuals as per chap. III of the GDPR (information, access, rectification and erasure, data portability, objection as well as automated individual decision-making) at any time and within the legal deadlines and will submit all necessary information to the client. Should a relevant request be sent to the contractor and should this request show that the sender of the request mistakenly considers him the controller of the processing operated by the contractor, then the contractor must forward this request to the client without delay and notify the sender of the above.
5. The contractor supports the client with adhering to the obligations, as outlined in Art. 32 to 36 GDPR (data security, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, prior consultation).
6. The contractor is made aware, that he must maintain a record of processing activities for the data processing in question in accordance with Art. 30 GDPR.
7. With regard to the provided data, the client is entitled to view and check the data processing facilities at any time, whether in person or via a commissioned third party. The contractor is obligated to provide the client with all necessary information to monitor the compliance with the obligations as outlined in this agreement.
8. Following the termination of this agreement, the contractor is obligated to forward to the client or destroy, at his request, all processing results and documents that contain data[[1]](#footnote-1). If the contractor should process the data in a unique, technical format then he is obligated to submit the data in this format, or, if requested by the client, in the format in which he received the data from the client or in another, common format, following the termination of this agreement.
9. The contractor must inform the client immediately, if he is of the opinion that an instruction of the client constitutes a violation of the data protection regulations of the Union or of the Member States.

# Place of performance of data processing

All data processing is exclusively executed in Austria.

# sub-Processors[[2]](#footnote-2)

{Prohibition on engaging a sub-processor} The contractor is not allowed to engage a sub-processor.

{Admissibility of engaging a specific sub-processor} The contractor is entitled to engage the following company as a sub-processor: [*edit company name and location, type of activity*].

Intended changes of the sub-processor are to be communicated to the client in such a timely manner, that the latter can forbid it. The contractor enters into an arrangement with the sub-processor in accordance with Art. 28 para. 4 GDPR. In doing so, he must ensure that the sub-processor adheres to the same obligations as the contractor, with regard to this agreement. Should the sub-processor not comply with his data protection obligations, then the contractor is liable vis-a-vis the client for the compliance with obligations of the sub-processor.

{Admissibility of engaging sub-processors} The contractor can employ sub-processors for [*activities*].

He must inform the client of the planned use of a sub-processor in such a timely manner, that the client can forbid it. The contractor enters into an arrangement with the sub-processor in accordance with Art. 28 para. 4 GDPR. In doing so, he must ensure that the sub-processor adheres to the same obligations as the contractor, with regard to this agreement. Should the sub-processor not comply with his data protection obligations, then the contractor is liable vis-a-vis the client for the compliance with obligations of the sub-processor.

|  |  |  |
| --- | --- | --- |
| [*place*], on [*date*] |  | [*place*], on [*date*] |
| *For the client:* |  | *For the contractor:* |
| ....................................................[Name and function] |  | ....................................................[Name and function] |

# Appendix ./1 - Technical-organiZational measures[[3]](#footnote-3)

## A. Confidentiality

**Entry control:** Avoidance of unauthorized entry to data processing facilities by:

|  |  |
| --- | --- |
| [ ]  Key | [ ]  Magnet or chip cards |
| [ ]  Electric door opener | [ ]  Doorman |
| [ ]  Security personnel | [ ]  Alarm system |
| [ ]  Video system | [ ]  Burglary-restraining windows and/or safety doors |
| [ ]  Registration at reception desk and identity check | [ ]  Follow-up of visitors on company premises |
| [ ]  Use of visitor or staff card/ID | [ ]  Other(s): |

**Access control:**

Avoidance of unauthorized system usage through:

|  |  |
| --- | --- |
| [ ]  Password (including relevant policies) | [ ]  Encryption of data carriers |
| [ ]  Automated locking mechanism | [ ]  Other(s): |
| [ ]  Two-factor authentication |  |

Avoidance of unauthorized reading, copying, changing or deleting within the system through:

|  |  |
| --- | --- |
| [ ]  Standard correction profile on a “need to know basis” | [ ]  Standard process for assigning authorisations |
| [ ]  Logging of access | [ ]  Safe storage of data carriers |
| [ ]  Regular checks of the assigned authorisations and of administrative user accounts in particular | [ ]  Privacy-compliant reuse of data carriers |
| [ ]  Privacy-compliant disposal of data carriers that are no longer needed. | [ ]  Clear-desk/clear-screen policy |
| [ ]  Other(s): |  |

**Pseudonymization:** If possible for the data processing operation, the primary identifiers are removed from within the data processing operation and saved elsewhere.

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

**Data classification scheme:** Based on legal obligations or self-assessment (secret/confidential/internal/public).

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

## B. Data Integrity[[4]](#footnote-4)

**Control of data transfer:** No unauthorised reading, copying, changing or deleting during electronic transfer or transport by way of:

|  |  |
| --- | --- |
| [ ]  Encryption of data carriers | [ ]  Encryption of data files |
| [ ]  Virtual private networks (VPN) | [ ]  Electronic signatures |
| [ ]  Other(s): |  |

**Data entry control:** Determination of whether and by whom personal data has been entered into the data processing system, changed or deleted by:

|  |  |
| --- | --- |
| [ ]  Logging | [ ]  Document management |
| [ ]  Other(s): |  |

## C. Availability and Resilience

**Availability control:** Protection against wilful destruction (negligent and/or wilful) or loss through:

|  |  |
| --- | --- |
| [ ]  Back-up strategy (online/offline; on-site/ off-site) | [ ]  Uninterrupted power supply (UPS, diesel generator) |
| [ ]  Virus protection | [ ]  Firewall |
| [ ]  Reporting channels and emergency procedures | [ ]  Security checks with regard to infrastructure and application |
| [ ]  Multi-level back-up approach with encrypted outsourcing of back-ups in a seperated data center | [ ]  Standard procedures for staff changes  |
| [ ]  Other(s): |  |

**Rapid** **recoverability**

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

## D. Procedures for regular testing, assessing and evaluating

**Data protection management**, including regular employee training courses:

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

**Incident response management**:

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

**Data protection by design**:

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

**Data processing control:** No data processing in the sense of Art. 28 GDPR without specific instruction by the client through:

|  |  |
| --- | --- |
| [ ]  Definitive contract design | [ ]  Formalized project management |
| [ ]  Strict selection of data processors (ISO-certified, ISMS) | [ ]  Due diligence |
| [ ]  Follow-up checks | [ ]  Other: |

1. Please delete as appropriate. [↑](#footnote-ref-1)
2. Please delete as appropriate. Sub-processors should also be based in Austria for this template. [↑](#footnote-ref-2)
3. Adapt according to the existing technical-organizational circumstances. [↑](#footnote-ref-3)
4. Prevention of (accidental) destruction, (accidental) damage, (accidental) loss, (accidental) changes of personal data. [↑](#footnote-ref-4)