[Bibliotheksname]

[Logo]

AUFTRAGSVERARBEITUNGSVERTRAG

gemäß Artikel 28 DSGVO

Abgeschlossen zwischen

[Bibliotheksname, Bibliotheksadresse]

bzw.

[Träger, Trägeradresse]

im Folgenden auch „**Verantwortlicher**“

und

[Name und Adresse des Auftragsverarbeiters/Dienstleisters]

im Folgenden auch „**Auftragsverarbeiter**“, gemeinsam kurz: „**die Parteien**“

**Inhalt**

[1. Begriffe 3](#_Toc516040850)

[2. Vertragsgegenstand 3](#_Toc516040851)

[3. Vertragsdauer 3](#_Toc516040852)

[4. Verarbeitungsgegenstand 4](#_Toc516040853)

[5. [Sonstige Bestimmungen] 6](#_Toc516040854)

[6. Anhang 1 – Datenanwendungen 7](#_Toc516040855)

[7. Anhang 2 – Technische und organisatorische Maßnahmen 8](#_Toc516040856)

AUFTRAGSVERARBEITERVERTRAG

**Hinweise zum Dokument:** Diese Vorlage soll Ihnen helfen, einen passenden Auftragsverarbeitervertrag z. B. mit ihrem Online-Diensteanbieter für einen WebOPAC oder für einen E-Medien-Verbund zu erstellen.

Folgende Punkte müssen **zwingend** enthalten sein:

* der Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters sowie gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
* der Name und die Kontaktdaten des Auftragsverarbeiters (Dienstleisters)
* Hinweis auf die DSGVO (Datenschutz-Grundverordnung-Auftragsverarbeitung nach Art 28 DSGVO)
* Gegenstand des Auftrags (Art und Zweck der Datenverarbeitung, detaillierte Beschreibung der Aufgaben des Auftragverarbeiters)
* Datenkategorien, die verarbeitet werden (z. B. Kontaktdaten, Vertragsdaten, Bestelldaten usw.)
* Kategorien betroffener Personen (z. B. LeserInnen, BenutzerInnen des Online-Dienstes, MitarbeiterInnen usw.)

# Begriffe

In diesem Auftragsverarbeitungsvertrag vorkommende Begriffe (z. B. personenbezogene Daten, betroffene Personen, Verarbeitung, Verletzung des Schutzes personenbezogener Daten, usw.) sind im Sinne der [Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016](http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE) (im Folgenden auch kurz „**DSGVO**“) auszulegen.

# Vertragsgegenstand

* 1. Der Verantwortliche steht mit dem Auftragsverarbeiter in einer Vertragsbeziehung, in deren Rahmen der Auftragsverarbeiter zum Zweck [Zweck einfügen] personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
  2. Der Verantwortliche beauftragt den Auftragsverarbeiter mit den im Anhang 1 aufgelisteten und beschriebenen Datenverarbeitungen (im Folgenden auch „**beauftragte Datenverarbeitungen**“).
  3. Anhang 1 beschreibt Gegenstand (Name der Anwendung), Zweck und die Art der beauftragten Datenverarbeitungen, ihre Speicherdauer, die dabei vom Auftragsverarbeiter verarbeiteten Kategorien betroffener Personen und die Arten verarbeiteter personenbezogener Daten.

# Vertragsdauer

Dieser Auftragsverarbeitungsvertrag gilt ab [Datum einfügen] und wird auf unbestimmte Zeit/befristet bis/für die einmalige Durchführung der Arbeiten abgeschlossen. Der Vertrag kann von beiden Parteien mit einer Frist von [Kündigungsfrist eintragen z. B. ein Monat] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

# Verarbeitungsgegenstand

Solange der Auftragsverarbeiter die Datenanwendung betreibt und personenbezogene Daten für den Verantwortlichen verarbeitet, gelten in Entsprechung des Art 28 DSGVO folgende Bedingungen:

* 1. Der Auftragsverarbeiter verpflichtet sich, sämtliche gesetzliche Vorgaben der Datenschutz-Grundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes (DSG) zu beachten und Datenanwendungen (logisch und physisch) ausschließlich innerhalb der EU oder des EWR zu betreiben. Jede Form der Verlagerung der Datenanwendung (dazu zählt auch die Verlegung des Sitzes des Auftragsverarbeiters) in ein Drittland (sohin außerhalb der EU oder des EWR) bedarf der schriftlichen, vorherigen Zustimmung durch den Verantwortlichen.
  2. Der Auftragsverarbeiter wird die Datenwendung wie vom Verantwortlichen schriftlich festgehalten verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
  3. Der Auftragsverarbeiter gewährleistet, dass sich Personen, die Kenntnis von den im Auftrag verarbeiteten Daten haben oder erhalten können, vor Verarbeitung bzw. Kenntnis dieser Daten schriftlich zur Vertraulichkeit verpflichten, sofern diese nicht ohnedies einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
  4. Der Auftragsverarbeiter wird geeignete technische und organisatorische Maßnahmen ergreifen um die Rechte und Freiheiten natürlicher Personen zu schützen. Dabei gilt es den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und den Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos zu berücksichtigen. Die Parteien werden diese Maßnahmen im Einvernehmen festlegen und evaluieren.
  5. Die Beauftragung bzw. Inanspruchnahme von Subauftragsverarbeitern (im Folgenden kurz: Subauftragnehmer) ist dem Auftragsverarbeiter prinzipiell gestattet, sofern er den Verantwortlichen vorab über jede beabsichtigte Beauftragung bzw. Inanspruchnahme von Subauftragnehmern schriftlich informiert und es dem Verantwortlichen freisteht, dieser Beauftragung bzw. Inanspruchnahme begründungslos zu widersprechen. Im Fall eines solchen Widerspruchs wird der Auftragsverarbeiter den Subauftragnehmer nicht beauftragen bzw. in Anspruch nehmen.

Der Auftragsverarbeiter ist verpflichtet, sämtliche Subauftragsnehmer im Sinne des Art 28 Abs 4 DSGVO schriftlich im Sinne dieses Vertrags zu verpflichten. Dabei ist sicherzustellen, dass der Subauftragsverarbeiter sämtliche Verpflichtungen eingeht, die dem Auftragnehmer aufgrund dieser Vereinbarungen obliegen. Sollte der Subauftragnehmer seine Pflichten verletzen, haftet der Auftragsverarbeiter. Der Subauftragnehmer muss seine Niederlassung innerhalb der EU oder des EWR haben. Der Subauftragnehmer darf die Datenanwendung ausschließlich innerhalb der EU oder des EWR betreiben. Die Beauftragung bzw. Inanspruchnahme von weiteren Subunternehmern durch den Subauftragnehmer ist dem Subauftragnehmer nur unter den im Punkt 4.5. festgesetzten Voraussetzungen gestattet.

* 1. Der Auftragsverarbeiter wird den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, damit dieser seine Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (Auskunft, Berichtigung und Löschung, Information, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Sollte sich ein Betroffener an den Auftragsverarbeiter oder einen Subauftragnehmer anstelle des Verantwortlichen wenden, verpflichten sich dieser, den Antrag dem Verantwortlichen unverzüglich zu senden, sodass der Verantwortliche den Antrag fristgerecht bearbeiten kann. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Ergreifung technischer und organisatorischer Maßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Erstellung einer Datenschutzfolgenabschätzung) unterstützen.
  2. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
  3. Der Auftragsverarbeiter wird nach Abschluss der Datenanwendung alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder vernichten/ löschen oder in einem gängigen elektronischen Format übergeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
  4. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der dem Auftragsverarbeiter in diesem Vertrag auferlegten Pflichten zur Verfügung zu stellen.
  5. Der Verantwortliche ist berechtigt, die Einhaltung sämtlicher maßgeblichen datenschutzrechtlichen Vorschriften sowie die Einhaltung der vertraglichen Bestimmungen selbst oder durch Dritte beim Auftragsverarbeiter sowie allfälligen Subauftragnehmern zu kontrollieren.
  6. Sollte der Auftragsverarbeiter der Auffassung sein, dass eine vom Verantwortlichen erteilte Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder deren Mitgliedstaaten verstößt, so hat er dies dem Verantwortlichen unverzüglich und begründet mitzuteilen.
  7. Dieser Vertrag erlangt durch die Unterfertigung oder eine schriftliche Bestätigung der Parteien Geltung.

# Sonstige Bestimmungen (optional, kann entfallen)

* 1. Diese Auftragsverarbeitungsvereinbarung unterliegt österreichischem Recht unter Ausschluss von Verweisnormen.
  2. Gerichtsstand ist das örtlich und sachlich zuständige Gericht am Sitz des Verantwortlichen.
  3. Sollte eine Bestimmung in diesem Auftragsverarbeitervertrag unwirksam oder undurchführbar sein oder werden, berührt dies die Wirksamkeit ihrer übrigen Bestimmungen nicht und wird durch eine neue wirksame Regelung ersetzt.

Für den Verantwortlichen Für den Auftragsverarbeiter

|  |  |  |
| --- | --- | --- |
|  |  |  |

Dieses Dokument wurde auf Basis der [WKO-Vorlage](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html) erstellt und erweitert; Anwaltliche Beratung durch: Mag. Markus Dörfler, Rechtsanwalt und Partner der Kanzlei Höhne, In der Maur & Partner Rechtsanwälte, [www.h-i-p.at](http://www.h-i-p.at/)und [datenschutz-recht.at](https://datenschutz-recht.at/). Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung des Büchereiverbandes Österreichs ist ausgeschlossen. Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter.

# Anhang 1 – Datenanwendungen[[1]](#footnote-1)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name der Anwendung | Zweck der Anwendung | Datenkategorien | Betroffenenkreis | Zugriff von | Empfänger (Auftragsverarbeiter) | Rechtsgrundlage | sensible Daten (x=Ja) | Speicherdauer | Maßnahmen zur Datensicherheit |
|  |  |  |  |  |  |  |  |  |  |

# Anhang 2 – Technische und organisatorische Maßnahmen

## Vertraulichkeit

* **Zutrittskontrolle:**Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z. B. Schlüssel
* **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z. B. Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Datenträgern
* **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, nur Zugriff von berechtigten Personen, Protokollierung von Zugriffen, regelmäßige Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten
* **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt
* **Klassifikationsschema für Daten:**Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (Kategorien: geheim/vertraulich/intern/öffentlich)

## Integrität[[2]](#footnote-2)

* **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
* **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B. Protokollierung, Dokumentenmanagement

## Verfügbarkeit und Belastbarkeit

* **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B. Backup-Strategie (online/offline), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
* Rasche **Wiederherstellbarkeit**
* **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles udgl.

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

* Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen
* Datenschutzfreundliche Voreinstellungen
* **Auftragskontrolle:**Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters), Vorabüberzeugungspflicht, Nachkontrollen

1. Bitte klären Sie mit Ihrem Auftragsverarbeiter, welche Datenanwendungen zu welchem Zweck in Auftrag gegeben werden. Besprechen Sie gemeinsam welche technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten ergriffen werden sollen. Die ausgewählten Maßnahmen müssen in das „Maßnahmen zur Datensicherheit“ eingefügt werden. Im Anhang 2 find Sie dafür einige Beispiele. [↑](#footnote-ref-1)
2. Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten. [↑](#footnote-ref-2)