# Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

**Vereinbarung**

zwischen der

Generaldirektion der Staatlichen Archive Bayerns

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

.........................

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## 1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus....................... (im Folgenden Leistungsvereinbarung).

(2) Dauer

Der Auftrag wird zur Durchführung der Leistungsvereinbarung erteilt und endet mit der Abnahme.

## 2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten   
Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:..................... Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien): Beispielsweise: Beschreibende Metadaten und Primärdaten zu Inhalt, Lagerung, Nutzung und Beschaffenheit des Archivgutes gem. Art. 2 BayArchivG und § 7 BArchG sowie den Archivbenützer\*innen gem. Art 10 BayArchivG und § 10 BArchG. Diese Meta- und Primärdaten können personenbezogene Daten, datenschutzrechtlich gesperrte Daten sowie unter einem besonderen gesetzlichen Geheimnisschutz (Steuergeheimnis, Sozialgeheimnis u.a.) stehende Daten ohne VS-Einstufung enthalten. Dazu gehören u. a. Daten zu Gesundheitszustand, Kommunikationsdaten, Vertragsstammdaten, Personenstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten, Auskunftsangaben sowie personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder aus denen die sexuellen Orientierung einer natürlichen Person hervorgeht.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen alle im digitalen Archivgut und den elektronischen Verzeichnungsdatensätzen der Staatlichen Archive Bayerns genannten Personen sowie die Mitarbeiterinnen und Mitarbeiter der Staatlichen Archive Bayerns und der Archivbenützer\*innen, die mit diesen Daten gearbeitet haben oder deren Einsicht beantragt haben.

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.

## 4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich zur Wahrnehmung seiner Rechte und Freiheiten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Als Ansprechpartner beim Auftragnehmer wird............... benannt.
2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO: Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet, zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht sowie über die zivil- und strafrechtlichen Folgen eines Verstoßes gegen Datenschutz und Vertraulichkeit belehrt wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
7. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
8. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 6. Unterauftragsverhältnisse

(1) Eine Unterbeauftragung ist unzulässig.

## 7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(2) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolgt durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO.

## 8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder nach entsprechender Vereinbarung mit dem Auftraggeber (Leistungsbeschreibung!) hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

# Anlage 1 – Technisch-organisatorische Maßnahmen

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

* Der Auftragnehmer stellt sicher, dass nur die mit der Leistungserbringung beauftragten Beschäftigten Zutritt zu den dafür verwendeten Datenverarbeitungsanlagen haben. Diese sind in eigenen Räumlichkeiten untergebracht, durch geeignete Schließanlagen gesichert und stets verschlossen zu halten. Arbeiten innerhalb der Räumlichkeiten mit den Datenverarbeitungsanlagen erfordern die Aufsicht durch befugtes Personal des Auftraggebers. Das Gebäude, in dem die betroffenen Datenverarbeitungsanlagen untergebracht sind ist alarmgesichert.
* Der Auftragnehmer stellt eine Zugangskontrolle sicher, um eine unbefugte Systembenutzung zu unterbinden.
* Der Auftragnehmer stellt innerhalb des datenverarbeitenden Systems und für die Verwendungszeit mobiler Datenträger durch den Einsatz von Berechtigungskonzepten sowie das Setzen von bedarfsgerechten Zugriffsrechten die Zugriffskontrolle in der Form sicher, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des datenverarbeitenden Systems und der genutzten mobilen Datenträger erfolgen kann.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

* Der Auftragnehmer kontrolliert die Weitergabe der zu verarbeitenden Daten unter den zuständigen Mitarbeiterinnen und Mitarbeitern und schützt zu übertragende Daten, um unbefugtes Lesen, Kopieren, Verändern oder Entfernen zu unterbinden.
* Der Auftragnehmer regelt die Eingabekontrolle durch personenbezogene Zugriffsrechte und dokumentiert diese, um nachweisen zu können,   
  ob und in welcher Weise und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

* Im Rahmen der Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) sichert der Auftragnehmer die eingesetzten Datenverarbeitungsanlagen. Die eingesetzten Datenverarbeitungsanlagen sind gegenüber dem Intranet und Internet durch ein aktuelles Virenschutzprogramm, den aktuellesten Patchstand und eine Firewall zu schützen. Über sicherheitsrelevante Vorfälle ist der Auftraggeber umgehend zu informieren und ggf. Anzeige bei der zuständigen Polizeidienststelle zu erstatten.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

* Der Auftragnehmer wendet datenschutzfreundliche Voreinstellungen in Form geeigneter technischer und organisatorischer Maßnahmen bei der Datenverarbeitung an, um sicherzustellen, dass personenbezogene Daten nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden (Art. 25 Abs. 2 DS-GVO).
* Die Wirksamkeit aller zum Datenschutz ergriffenen Maßnahmen ist im Rahmen eines Datenschutz-Management in regelmäßigen Abständen, mindestens aber einmal im Monat durch den Auftragnehmer zu überprüfen.
* Für alle Verletzungen des Datenschutzes ist ein fester Meldeweg mit konkreten Handlungsanweisungen zur Unterbindung einer weiteren Verletzung des Datenschutzes für die Beschäftigten des Auftragnehmers zu implementieren.
* Es darf keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers erfolgen.

München, den \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , den \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Auftraggeber Auftragnehmer