

Anlage 2:
Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend die OZG-Verwaltungsleistung:

Einbürgerung (OZG-ID: 10257)

Zwischen dem Auftraggeber (Leistungsbezieher) und dem Auftragnehmer (Leistungserbringer, Kommunalvertreter) wird mit Vertragsschluss des Einzelabrufs die folgende Einzel-Auftragsvereinbarung (nachstehend „Einzel-AV“) zum Einzelabruf betreffend die OZG-Verwaltungsleistung „Einbürgerung“ als Anlage 2 (nachstehend „Einzelabruf“) geschlossen.

Präambel

Diese Einzel-AV regelt auf Grundlage der zwischen den Vertragsparteien geschlossenen Rahmenvereinbarung zur Auftragsverarbeitung (nachstehend „**Rahmen-AV**“) die Einzelheiten der Datenverarbeitung im Zusammenhang mit dem Einzelabruf „Einbürgerung“.

1 OZG-Verwaltungsleistungs-spezifische Zwecke, Betroffene und Datenkategorien

Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Einbürgerung“ personenbezogene Daten zu folgenden Zwecken, von folgenden Betroffenen und mit folgenden Datenkategorien:

I. Zwecke

Der Zweck des Online-Dienstes ist die elektronische Beantragung eines Einbürgerungsantrages.

Der Online-Dienst bildet dabei die folgenden Unterzwecke ab:

- a. Vorabauskunft, ob die Beantragung für die Person in Frage kommt,
- b. Strukturierte elektronische Erhebung von Antragsdaten, ggf. unter Zuhilfenahme des Nutzerkontos (Übergabe der dort hinterlegten Stamm- und Kontaktdaten),
- c. Übermittlung der Antragsdaten zur Weiterbearbeitung im Fachverfahren,

II. Betroffene

Betroffene sind:

- Antragsteller: Ausländerinnen und Ausländer im Sinne des Staatsangehörigkeitsgesetzes (StAG) bzw. Staatenlose als Nutzende des Online-Dienstes (Antragsteller), Personen die als Bevollmächtigte einen Antrag stellen;
- Angehörige der Antragsteller wie Ehepartner oder minderjährige Kinder, falls diese über den gleichen Antrag miteingebürgert werden sollten.

III. Datenkategorien

Kategorien der Daten, die immer verarbeitet werden:

Vorname, Familienname, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, Familienstand, Geschlecht, Adressdaten, Zahlungsinformationen.

Folgende Kategorien werden nur bei Bedarf verarbeitet:

Daten zu wirtschaftlichen Verhältnissen, Daten zum ausländerrechtlichen Status, Schulbildung, Sprachkenntnisse, Personendaten von Vorfahren, Ehegatten und Kindern, frühere Personendaten, Volkstum.

Besondere Kategorien personenbezogener Daten („sensible Daten“), Verarbeitung nur falls für das spezielle Verfahren erforderlich:

Daten zur Verurteilung wegen einer Straftat, Daten aus den Ermittlungsergebnissen der angefragten Behörden, Gesundheitsdaten, Daten zur politischen Orientierung soweit sie sich aus der erforderlichen Sicherheitsbefragung und/oder der Ausländerakte ergeben.

2 Technische und organisatorische Maßnahmen (TOM)

Technische und Organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO (unter Einhaltung sonstiger relevanter gesetzlicher Vorschriften und AKDB-interner Compliance-Regelungen) für im AKDB-Rechenzentrum betriebene Verfahren. Als Nachweis des Stands der Technik hält die AKDB ein BSI-Zertifikat vor.

Die regelmäßige Überprüfung der Wirksamkeit der Technischen und Organisatorischen Maßnahmen erfolgt mindestens jährlich im Rahmen der vorhandenen ISO 27001-Zertifizierung auf Basis von BSI IT-Grundschutz.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

- Mehrstufigen Zutrittsschutz
 - Besucherkontrolle am Empfang am Standort des Primärrechenzentrums
 - Gesonderte Zutrittsberechtigung zu allen sicherheitsrelevanten Räumen mittels Chipkarte und zusätzlicher Codeeingabe am Zugangsterminal
- Regelmäßige Überprüfung der Zutrittsberechtigungen
- Kontrollierte Schlüsselvergabe
- Videoüberwachung des Gebäudes einschließlich des Zugangs sowie in den Storage- und CPU-Räumen im Primärrechenzentrum
- Außenhautsicherung des Primärrechenzentrumgebäudes an kritischen Stellen durch einbruchhemmende Spezialfenster und Türen
- Außenhautsicherung des Primärrechenzentrumgebäudes kombiniert mit Einbruchmeldeanlage mit Alarmweiterleitung zur Polizei
- Besucher in Begleitung durch Mitarbeiter

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Login mit Benutzername und Passwort
- Detaillierte Passwortregelung
- Erzwungene Passwortkomplexität
- Regelmäßigen technisch vorgegebenen Passwortwechsel
- Sperrung der Benutzererkennung nach mehrmaliger Fehleingabe
- Detaillierte Security-Policies für die Produktionsumgebung und deren regelmäßige Überprüfung
- Einsatz von Firewall-Systemen mit eigener Security-Policy
- Zusätzlicher Einsatz von Intrusion-Prevention-Systemen
- Anti-Viren-Software
- Mobile Device Management
- Verschlüsselung von Notebooks

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Regelmäßige Aktualisierung der Sicherheitskonzepte
- Vergabe differenzierter Berechtigungsstufen innerhalb der Verfahren
- Protokollierung von Veränderungen oder Löschungen der Daten
- Datenträgervernichtung gemäß DIN 66399

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Datenübermittlung über gesicherte Datenverbindungen
- Verschlüsselung der Daten beim Transport auf Datenträgern

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Anlage 2: Auftragsverarbeitung zum Einzelabruf „Einbürgerung“ und technisch-organisatorische Maßnahmen (TOM)

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Keine Modifizierbarkeit der Protokolle
- Kontrolle der Protokolle

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Hohe Hardwarequalität der Systeme mit abgeschlossenen Wartungsverträgen mit kurzen Reaktionszeiten seitens der Hardwarehersteller
- Redundante Server-Systeme
- Speicherung der Daten auf eigenen Storage-Systemen mit Raid-Technik und Spareplatten, zu großen Teilen in Clustertechnik ausgeführt
- Aufbewahrung von längerfristigen Sicherungsbeständen im Tresor
- Regelmäßig aktualisierten Virenschutz
- Redundante Firewall-Systeme
- Redundante Internetanschlüsse
- Redundanter Behördennetzanschluss (BYBN)
- Mobile Arbeitsplätze mit gesichertem Zugang für Mitarbeiter in den Bereichen Operating, Produktionsdurchführung und Systemadministration zum Zugang auch außerhalb der üblichen Arbeitszeiten
- Gebäudetechnische Maßnahmen (Feuer- Rauchmeldeanlagen, Feuerlöscher, Klimatisierung, USV)
- Regelmäßiges Patchen der Systeme (Funktions- und Sicherheitspatches)
- Regelmäßige Backup- und Recovery-Maßnahmen
- Regelmäßige Tests zur Datenwiederherstellung

3 Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Kontaktperson	Anschrift	Leistung
1	AKDB	Michael Diepold Martin Senft	Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) Hansastraße 12-16 80686 München	Betrieb der virtuellen Container-Infrastruktur für die eigentliche Anwendung und die dazu benötigten Dienste (Anwendungscluster) sowie Betrieb der OK.KOMM-Schnittstelle für den Online-Dienst