

Eigenerklärung Datenschutzrecht

Eigenerklärung zur Einhaltung des Datenschutzrechts

Im Rahmen der Leistungserbringung wird eine Auftragsverarbeitung erfolgen, d.h. es werden durch den künftigen Auftragnehmer personenbezogene Daten verarbeitet.

Der Bedarfsträger wird als Verantwortlicher für diese Auftragsverarbeitung rechtzeitig vor Leistungserbringung die Vereinbarung zur Auftragsverarbeitung mit dem künftigen Auftragnehmer abschließen.

Der künftige Auftragnehmer ist verpflichtet seine innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind geeignete technische und organisatorische Maßnahmen (TOM) zu treffen und so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

Zum Nachweis, dass Sie als Bieter die Anforderungen zum Datenschutz erfüllen und die Einhaltung durch technische und organisatorische Maßnahmen (TOM) sicherstellen, verlangt die Vergabestelle von Ihnen die nachfolgende Eigenerklärung. Sie wird bei Zuschlag Bestandteil der Vereinbarung zur Auftragsdatenverarbeitung.

Hiermit verpflichte ich mich/verpflichten wir uns, die jeweils geltenden Datenschutzbestimmungen zu beachten und die sich hieraus ergebenden Verpflichtungen einzuhalten.

Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

I. Unter Berücksichtigung der Art der vorliegend zu schützenden personenbezogenen Daten und Datenkategorien (vgl. Vereinbarung zur Auftragsverarbeitung) werden folgende Maßnahmen getroffen, die geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
 - ☐ Alarmanlage,
 - ☐ Absicherung von Gebäudeschächten,
 - ☐ automatisches Zugangskontrollsystem,
 - ☐ Chipkarten-/Transponder-Schließsystem,
 - ☐ Schließsystem mit Codesperre,
 - ☐ manuelles Schließsystem,
 - ☐ biometrische Zugangssperren,
 - ☐ Videoüberwachung der Zugänge,
 - ☐ Lichtschranken/Bewegungsmelder,
 - ☐ Sicherheitsschlösser,
 - ☐ Schlüsselregelung (Schlüsselausgabe etc.),
 - ☐ Personenkontrolle beim Pförtner/Empfang,
 - ☐ Protokollierung der Besucher,
 - ☐ sorgfältige Auswahl von Reinigungspersonal,

- ☐ sorgfältige Auswahl von Wachpersonal,
- ☐ Tragepflicht von Berechtigungsausweisen,
- ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können
(Zugangskontrolle),

- ☐ Zuordnung von Benutzerrechten,
- ☐ Erstellen von Benutzerprofilen,
- ☐ Passwortvergabe,
- ☐ Authentifikation mit biometrischen Verfahren,
- ☐ Authentifikation mit Benutzername/Passwort,
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen,
- ☐ Gehäuseverriegelungen,
- ☐ Einsatz von VPN-Technologie,
- ☐ Sperren von externen Schnittstellen (USB etc.),
- ☐ Sicherheitsschlösser,
- ☐ Schlüsselregelung (Schlüsselausgabe etc.),
- ☐ Personenkontrolle beim Pförtner/Empfang,
- ☐ Protokollierung der Besucher,
- ☐ sorgfältige Auswahl von Reinigungspersonal,
- ☐ sorgfältige Auswahl von Wachpersonal,
- ☐ Tragepflicht von Berechtigungsausweisen,
- ☐ Einsatz von Intrusion-Detection-Systemen,
- ☐ Verschlüsselung von mobilen Datenträgern,
- ☐ Verschlüsselung von Smartphone-Inhalten,
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten),
- ☐ Einsatz von Anti-Viren-Software,
- ☐ Verschlüsselung von Datenträgern in Laptops/Notebooks,
- ☐ Einsatz einer Hardware-Firewall,
- ☐ Einsatz einer Software-Firewall,
- ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

3. zu 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 (**Zugriffskontrolle**),
- ☐ Einsatz von Berechtigungskonzepten,
 - ☐ Verwaltung der Rechte durch Systemadministratoren,
 - ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert,
 - ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel,
 - ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten,
 - ☐ sichere Aufbewahrung von Datenträgern,
 - ☐ physische Löschung von Datenträgern vor Wiederverwendung,
 - ☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757),
 - ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel),
 - ☐ Protokollierung der Vernichtung,
 - ☐ Verschlüsselung von Datenträgern,
 - ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

4. zu 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 einer Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln,
 - ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form,
 - ☐ E-Mail-Verschlüsselung,
 - ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen,
 - ☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen,
 - ☐ beim physischen Transport: sichere Transportbehälter/-verpackungen,
 - ☐ Sorgfalt bei Auswahl von Transportpersonal und -fahrzeugen,
 - ☐ Persönliche Übergabe mit Protokoll,
 - ☐ Protokollierung der Zugriffe und Abrufe,
 - ☐ Nutzung von Signaturverfahren,
 - ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingangs-/Eingabekontrolle**),

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten,
- ☐ Manuelle oder automatische Kontrolle der Protokolle,
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Programmen welche Daten eingegeben, geändert und gelöscht werden können,
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen),
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind,
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts,
- ☐ Klare Zuständigkeiten für Löschungen,
- ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

6. zu gewährleisten, dass personenbezogene Daten, die im Rahmen eines Unterauftragsverhältnisses verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

- ☐ Auswahl des Unterauftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit),
- ☐ vorherige Prüfung der und Dokumentation der beim Unterauftragnehmer getroffenen Sicherheitsmaßnahmen,
- ☐ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung,
- ☐ schriftliche Weisungen an den Unterauftragnehmer,
- ☐ Verpflichtung der Mitarbeiter des Unterauftragnehmers auf das Datengeheimnis,
- ☐ Unterauftragnehmer hat Datenschutzbeauftragte/n bestellt,
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags,
- ☐ wirksame Kontrollrechte gegenüber dem Unterauftragnehmer vereinbart,
- ☐ Regelung zum Einsatz weiterer Subunternehmer,
- ☐ laufende Überprüfung des Unterauftragnehmers und seiner Tätigkeiten,
- ☐ Vertragsstrafen bei Verstößen,
- ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

- ☐ Unterbrechungsfreie Stromversorgung (USV),
- ☐ Klimaanlage in Serverräumen,
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen,
- ☐ Schutzsteckdosenleisten in Serverräumen,
- ☐ Feuer- und Rauchmeldeanlagen,
- ☐ Feuerlöschgeräte in Serverräumen,
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen,
- ☐ Erstellen eines Backup- & Recoverykonzepts,
- ☐ Kontrolle des Sicherungsvorgangs
- ☐ Aufbewahrung der Sicherungssysteme an einem sicheren Ort außerhalb des Serverraums
- ☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse,
- ☐ Erstellen eines Notfallplans,
- ☐ RAID System/ Festplattenspiegelung
- ☐ Serverräume nicht unter sanitären Anlagen,
- ☐ in Hochwassergebieten: Serverräume über der Wassergrenze,
- ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (**Trennungsgebot**).

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern,
- ☐ logische Mandantentrennung (softwareseitig),
- ☐ Steuerung über Berechtigungskonzept,
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden,
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern,
- ☐ bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System,
- ☐ Festlegung von Datenbankrechten,
- ☐ Trennung von Produktiv- und Testsystem,
- ☐ sonstige Maßnahmen:

(ggf. auf gesonderter Anlage)

II. ☐ Ich/wir verpflichte/n folgende Unterauftragnehmer zur Übernahme von Leistungsbestandteilen, bei denen eine Auftragsverarbeitung stattfindet:

(Hinweis: Es sind die Unternehmensbezeichnung, die vollständige Adresse sowie die übertragenen Aufgaben anzugeben.)

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

☐ weitere Unterauftragnehmer (auf gesonderter Anlage)

alternativ:

☐ Hiermit versichere ich/versichern wir, keine Unterauftragnehmer im Sinne einer Auftragsverarbeitung einzusetzen.

Mir/uns ist bewusst, dass wissentlich falsche Angaben in den vorstehenden Erklärungen
- meinen/unseren Ausschluss von der Auftragserteilung gemäß § 124 Abs. 1 Nr. 8 GWB
- eine fristlose Kündigung des Vertrages
zur Folge haben können.

Bieter:	
Unterschrift:	