

Selbstauskunft.

Selbstauskunft.

(zu den Maßnahmen nach Art. 32 DS-GVO).

Name des Auftragnehmers

Anschrift: Straße u. Hausnummer

Anschrift: PLZ u. Ort

Für die Beurteilung der Datenschutzorganisation des Auftragnehmers sind die nachfolgenden Auskünfte erforderlich. Die Angaben sind wahrheitsgemäß und in dem Umfang zu machen, der für eine Beurteilung der Maßnahmen durch den Auftraggeber notwendig ist.

(Es sind nur die für die Auftragsverarbeitung relevanten Punkte auszufüllen)

Datenschutzrecht/Aufsichtsbehörde

Welches Datenschutzrecht findet beim Auftragnehmer Anwendung (DS-GVO, BDSG, LDSG) und welche Aufsichtsbehörde ist für den Auftragnehmer zuständig (Bezeichnung und Anschrift)?

Beauftragter für den Datenschutz

Wurde ein Beauftragter für den Datenschutz gemäß Art. 37 DS-GVO schriftlich bestellt und werden vom diesem die in Art. 39 DS-GVO beschriebenen Aufgaben wahrgenommen?

☐ ja ☐ nein

Name, Vorname und Anschrift des Datenschutzbeauftragten:

Selbstauskunft.

Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

Getroffene Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

1.1. Wo erfolgt die Verarbeitung von personenbezogenen Daten des Auftraggebers (z. B. Büroräume, Rechenzentrum, Cloud)?

1.2. Durch welche Maßnahmen werden die Gebäude gesichert?

1.3. Mit welchen Maßnahmen wird der Zutritt zu den Räumlichkeiten gesichert?

1.4. Mit welchen Maßnahmen wird der Zutritt zu den besonders schützenswerten Räumlichkeiten gesichert?

1.5. Werden die Zutrittsberechtigungen dokumentiert?

1.6. Gibt es ein dokumentiertes Verfahren für die Vergabe / Entzug von Zutrittsberechtigungen?

1.7. Welche Regelungen wurden zum Gebäudezutritt von Firmenfremden / Gästen / Besuchern getroffen?

1.8. Welche Regelungen wurden zum Gebäudezutritt von Reinigungs- und Wartungspersonal getroffen?

1.9. Bestehen dokumentierte Verfahren bzgl. der Entziehung von Gebäudezutrittsberechtigungen und Zugriffsrechten zu Computersystemen für Mitarbeiter bei Beendigung des Arbeitsverhältnisses?

Selbstauskunft.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

2.1. Wie wird das Firmennetzwerk gegen das öffentliche Netzwerk geschützt (z. B. Firewall, E-Mail Gateway)?

2.2. Werden Mobile Device Management Anwendungen für die Verwaltung mobiler Geräte eingesetzt?

2.3. Werden regelmäßig Penetrationstests durchgeführt? Datum des letzten Pentests.

2.4. Ist eine Passwort-Richtlinie umgesetzt worden? Bitte erläutern.

2.5. Wie werden den Mitarbeiter Zugangsberechtigungen zugewiesen? Bitte erläutern oder auf gesondert beigelegte Dokumente verweisen.

2.6. Werden die Zugangsberechtigungen dokumentiert?

2.7. Wie oft findet eine Prüfung der Zugangsberechtigungen statt?

2.8. Wird der administrative Account ausschließlich für administrative Tätigkeiten eingesetzt?

2.9. Werden Administrationspasswörter für IT-Systeme gesichert aufbewahrt?

2.10. Werden alle mobilen Geräte nach dem aktuellen Stand der Technik verschlüsselt?

Selbstauskunft.

2.11. Werden Virens Scanner auf allen Servern / Clients / mobilen Geräte eingesetzt? Wenn ja, wie regelmäßig erfolgt die Aktualisierung?

2.12. Sind Regelungen implementiert, die erläutern, wie im Falle von Warnmeldungen zu verfahren ist? Werden diese zentral erfasst?

2.13. Werden sicherheitsrelevante Softwareupdates regelmäßig und automatisiert eingespielt?

2.14. Welche Regelungen wurden bezüglich des Internetzugangs getroffen (Whitelisting / Blacklisting pro Usergruppe, Firewallregeln)?

3. Zugriffskontrolle

Auftragnehmer gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigte 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.

3.1. Sind Datenträger vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen geschützt?

3.2. Werden Berechtigungen für den Zugriff auf Anwendungen und Daten nach dem „Need-to-know-Prinzip“ vergeben und sind diese dokumentiert?

3.3. Wer genehmigt die Zugriffsberechtigungen auf Anwendungen und Daten?

3.4. Wie oft findet die Prüfung der Zugriffsberechtigungen statt?

3.5. Wie werden Arbeitsplatzrechner und mobile Geräte gegen externe Datenspeicherung gesichert?

Selbstauskunft.

3.6. Werden externe Zugriffe für Mitarbeiter und Betriebsfremde (Auftraggeber / Dienstleister) auf das Firmennetzwerk ermöglicht?

3.7. Welche Regelungen wurden hinsichtlich Remote-Zugriffen getroffen?

3.8. Werden Daten des Auftraggebers außerhalb der Betriebsräume des Auftragsverarbeiters verarbeitet und in welcher Form? (z. B. Telearbeit, mobiles Arbeiten, Home-Office)

3.9. Sind Regelungen getroffen worden, um die Datenschutzgrundsätze außerhalb der Betriebsräume sicherzustellen? Bitte erläutern oder auf gesondert beigefügte Dokumente verweisen.

3.10. Ist die Nutzung von BYOD erlaubt? Wenn ja, welche Regelungen zum Schutz der Daten des Auftraggebers wurden in diesem Zusammenhang getroffen? Bitte erläutern oder auf gesondert beigefügte Dokumente verweisen.

3.11. Wie erfolgt die Vernichtung von Datenträger und Papierdokumenten? Nach welcher Norm und Stufe?

4. Trennungskontrolle

Der Auftragnehmer gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

4.1. Welche Maßnahmen zur Mandantentrennung wurden ergriffen?

4.2. Ist ein Berechtigungskonzept für die relevanten Anwendungen und Datenbestände, welches den Zugriff durch projektfremde Mitarbeiter auf die Daten ausschließt, vorhanden und umgesetzt worden?

4.3. Werden Mitarbeiter schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte / Zwecke miteinzubringen?

Selbstauskunft.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Der Auftragnehmer gewährleistet, dass die Daten so aufbereitet werden, dass ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

5.1. Werden Daten des Auftraggebers pseudonymisiert? Bitte erläutern.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

6. Weitergabekontrolle

Der Auftragnehmer gewährleistet, 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 Einrichtung zur Datenübertragung vorgesehen ist.

6.1. Werden Daten mittels Datenträger zwischen dem Auftraggeber und Auftragnehmer übermittelt? Bitte erläutern.

6.2. Sind die Daten bei der Abholung und beim Transport gegen unbefugten Zugriff und Verlust geschützt? Bitte erläutern.

6.3. Werden die Daten beim Auftragnehmer vernichtet? Wenn ja, welche Sicherheitsmaßnahmen sind für die Vernichtung eingerichtet worden?

6.4. Werden Daten auf dem elektronischen Wege zwischen dem Auftraggeber und Auftragnehmer übermittelt? Bitte erläutern.

6.5. Werden personenbezogene Daten per E-Mail übermittelt? Wie wird der Übermittlungsweg gesichert?

6.6. Werden Daten des Auftraggebers in der Cloud oder unter Hinzuziehung von Cloud-Services verarbeitet? Bitte erläutern.

Selbstauskunft.

6.7. Wie werden die Daten des Auftraggebers, bei Nutzen von Cloud-Services, vor unbefugtem Zugriff geschützt? (bspw. Verschlüsselung etc.) Bitte um Nachweise.

6.8. Wie erfolgt nach der Datenübermittlung die Löschung der Daten des Auftraggebers (elektronisch und analog)?

6.9. Welche Schutzmaßnahmen wurden zum Schutz der Daten des Auftraggebers (auch temporär) auf mobilen Geräten getroffen?

7. Eingabekontrolle

Der Auftragnehmer gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

7.1. Werden Log-Files für die Nachvollziehbarkeit der Eingabe / Änderung / Löschung von Daten des Auftraggebers je Account angelegt?

7.2. Werden die Log-Files manuell gesichtet oder erfolgt eine automatisierte Kontrolle?

7.3. Existiert eine Anwendungsübersicht aus der hervorgeht, mit welchen Anwendungen welche Daten eingegeben, geändert oder gelöscht werden können?

7.4. Erfolgt die Vergabe von Rechten zur Eingabe / Änderung / Löschung von Daten auf Basis eines Berechtigungskonzepts?

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

8. Verfügbarkeitskontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8.1. Wie erfolgt die Datensicherung? Bitte erläutern.

Selbstauskunft.

8.2. Wurden die Maßnahmen in einem ausformuliertem Backup-Konzept festgehalten? Stand des Konzepts.

8.3. Wie regelmäßig finden Tests zur Datenwiederherstellung statt?

8.4. Durch welche technischen Maßnahmen ist der Datensicherungsort gegen Zerstörung gesichert (z. B. Feuer- und Rauchmeldeanlage, Serverraumüberwachung)?

8.5. Wie viele Tage beträgt die Wiederanlaufzeit des Rechenzentrums nach vollständiger Zerstörung?

8.6. Werden USVs für die Überbrückung bei Stromausfall und Spannungsschwankungen eingesetzt?

8.7. Ist für die Sicherstellung der Verfügbarkeit von IT-Systemen ein Notfallplan vorhanden und umgesetzt? Stand des Konzepts.

8.8. Wurden für die Wartung der IT-Systeme durch Externe AV-Verträge abgeschlossen?

8.9. Werden diese regelmäßig auditiert?

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

9. Auftragskontrolle

Auftragnehmer gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Selbstauskunft.

9.1. Werden die Unterauftragnehmer unter der Berücksichtigung der Sorgfaltsgesichtspunkte in Bezug auf den Datenschutz und Datensicherheit ausgewählt?

9.2. Bestehen mit Unterauftragnehmer, die Zugriff auf die Daten des Auftraggebers haben, Verträge zur Auftragsverarbeitung?

9.3. Gibt es Unterauftragnehmer außerhalb der EU, die Zugriff auf die Daten des Auftraggebers haben oder verarbeitet der Auftragnehmer diese außerhalb der EU?

9.4. Anhand welcher Rechtsgrundlage? (z.B. neuen Standardvertragsklauseln)

9.5. Halten die Unterauftragnehmer dasselbe Niveau der vereinbarten technischen und organisatorischen Maßnahmen, wie die des Auftragnehmers gegenüber dem Auftraggeber ein und wurde deren Einhaltung vertraglich zugesichert?

9.6. Wurden die bei der Datenverarbeitung beschäftigten Mitarbeiter der Unterauftragnehmer schriftlich auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und entsprechend belehrt?

9.7. Verfügt der Unterauftragnehmer über Sicherheitszertifizierungen bspw. nach ISO 27001, BSI IT-Grundschutz oder ISIS12? Bitte Nachweise beifügen.

9.8. Wurden Vereinbarungen zur Ausübung wirksamer Kontrollrechte gegenüber dem Unterauftragnehmer getroffen?

9.9. Falls die Dienstleistung unter Zuhilfenahme von Cloud-Services erbracht wird, bitte um Einreichung einer Übersicht, aus der die eingesetzten IT-Komponenten, Orte der Speicherung und die verwendeten Protokolle hervorgehen.

Selbstauskunft.

10. Datenschutzmanagement

10.1. Ist ein Datenschutzmanagement implementiert worden?

10.2. Sind Verarbeitungstätigkeiten, die vom Verantwortlichen durchgeführt werden, in einem Verzeichnis von Verarbeitungstätigkeiten dokumentiert?

10.3. Ist eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf vorhanden?

10.4. Es bestehen IT-Sicherheits- und Datenschutzkonzepte, die regelmäßig aktualisiert werden.

10.5. Ist ein Informationssicherheitsbeauftragte*r bestellt worden? Bitte um Angaben.

10.6. Wie regelmäßig findet eine Überprüfung der Wirksamkeit von technischen Schutzmaßnahmen statt? Bitte erläutern.

10.7. Wurden die bei der Datenverarbeitung beschäftigten Mitarbeiter schriftlich auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und entsprechend belehrt?

10.8. Finden für die Mitarbeiter regelmäßig Schulungen und Sensibilisierungsmaßnahmen zum Datenschutz statt? In welchem Zyklus?

10.9. Werden die außerhalb der Betriebsräume tätigen Mitarbeiter gesondert zur sicheren Nutzung von Home-Office Lösungen sensibilisiert und werden ihnen spezifische Gefahren aufgezeigt? Bitte erläutern.

11. Sonstiges

11.1. Liegt eine Sicherheitszertifizierung bspw. nach ISO 27001, BSI IT-Grundschutz oder ISIS12 vor? Bitte Nachweise beifügen.

Selbstauskunft.

11.2. Sind Prozesse zur Beantwortung von Auskunftsanfragen seitens der Betroffenen vorhanden?

11.3. Sind technische Maßnahmen implementiert, die eine einfache Ausübung des Widerrufsrechts des Betroffenen ermöglichen?

11.4. Existieren im Unternehmen des Auftragnehmers Regelungen zum Umgang mit Sicherheitsvorfällen? Bitte um Nachweise.

11.5. Sind der Datenschutz- und IT-Sicherheitsbeauftragten in die Prozesse der Sicherheitsvorfälle und Datenpannen eingebunden?

11.6. Werden Intrusion Detection Systeme eingesetzt?

11.7. Werden Intrusion Prevention Systeme eingesetzt?

Falls die Leistungen der Beauftragung auch die Bereitstellung von Diensten oder die Entwicklung von Software umfassen:

11.8. Existieren im Unternehmen Regelungen zum „Datenschutz durch Technikgestaltung“, um das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen?

11.9. Existieren im Unternehmen Regelungen zur Verwendung personenbezogener Daten in der Softwareentwicklung?

Selbstauskunft.

Wir versichern, dass die hier getätigten Angaben dem aktuellen Stand der bei uns umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten Angaben sind unmittelbar an den Auftraggeber zu melden.
