

Anlage 1: Allgemeine technische und organisatorische Maßnahmen
gem. Art. 32 DSGVO

data kulturlink ag
Rosenthaler Strasse 38, 10178 Berlin

(Stand: 1.9.2020)

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

a) Zutrittskontrolle

Durch die nachfolgenden Maßnahmen wird sichergestellt, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt ist:

(Beispiele: Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel / Schlüsselvergabe, Türsicherung (elektrische Türöffner usw.), Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Video- / Fernsehmonitor)

- | | |
|---|--|
| <input type="checkbox"/> Alarmanlage | <input type="checkbox"/> Absicherung von Gebäudeschächten |
| <input checked="" type="checkbox"/> Manuelles Schließsystem/ Sicherheitsschlösser | <input type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input checked="" type="checkbox"/> Schließsystem mit Codesperre | <input type="checkbox"/> Multifaktor Authentifizierung für den Zutritt zum Serverraum (Pin/ Karte) |
| <input type="checkbox"/> Videoüberwachung der Zugänge | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal |
| <input type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Besucher können nur in Begleitung von Mitarbeitern die Geschäftsräume betreten |

b) Zugangskontrolle

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

(Beispiele: sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Verwendung von Firewalls, Einrichtung eines Benutzerstammsatzes pro User)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen |
| <input type="checkbox"/> Passwortrichtlinie in einer IT-Richtlinie dokumentiert und per Policy in den IT-Systemen umgesetzt | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input checked="" type="checkbox"/> Verschlüsselung der Datenkommunikation auf der Webseite | <input type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen USB-Schnittstellen | <input type="checkbox"/> Sicherheitsschlösser |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Besucherkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Systemschutz durch Hardware-Firewall und Virens Scanner | <input type="checkbox"/> Protokollierung der Besucher |
| <input type="checkbox"/> Einsatz einer zentralen Smartphone-Administrations-Software (MDM) (z.B. zum externen Löschen von Daten) | <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Verschlüsselung von Datenträgern in mobilen Geräten | <input type="checkbox"/> Verschlüsselung der Datenkommunikation auf der Webseite und des externen Bewerbungsmanagementsystems |

c) Zugriffskontrolle / Benutzerkontrolle

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.

(Beispiele: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, Auswertungen Kenntnisnahme, Veränderung und Löschung)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input type="checkbox"/> Protokollierung von Zugriffen in Anwendungen insbesondere in SAP bei der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Ordnungsgemäße zertifizierte Vernichtung von Datenträgern |
| <input type="checkbox"/> Physische Löschung von Datenträgern vor Wiederverwendung | <input type="checkbox"/> Protokollierung der Vernichtung |
| <input type="checkbox"/> Einsatz von Aktenvernichtern und externen zertifizierten Dienstleistern | <input type="checkbox"/> _____ |

d) Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

(Beispiele: Mandantenfähigkeit / Zweckbindung, Sandboxing, Funktionstrennung / Produktion / Test)

- | | |
|--|---|
| <input type="checkbox"/> Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input type="checkbox"/> Logische Trennung mittels eigener logischer Buchungskreise |
| <input type="checkbox"/> Erstellung eines Berechtigungskonzepts | <input type="checkbox"/> Trennung von Produktiv- und Testsystemen |
| <input type="checkbox"/> Festlegung von Datenbankrechten | <input type="checkbox"/> _____ |

e) Maßnahmen zur Verschlüsselung der Daten

Maßnahmen zur Verschlüsselung von personenbezogenen Daten

(Beispiele: Verschlüsselung der E-Mail-Kommunikation, Festplattenverschlüsselung, Verschlüsselung von Datenbanken und Backupsystemen, Einsatz von VPN etc.)

- | | |
|---|--|
| <input type="checkbox"/> Transportverschlüsselung durch Einsatz von VPN-Technologie | <input type="checkbox"/> Verschlüsselung der E-Mail-Kommunikation |
| <input checked="" type="checkbox"/> Festplattenverschlüsselung | <input type="checkbox"/> Verschlüsselung der Datenkommunikation (SAP, Webseiten) |
| <input type="checkbox"/> Verschlüsselung von E-Mail Inhalten mittel ZIP-Archive (AES-256) | <input type="checkbox"/> _____ |

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

a) Weitergabekontrolle / Übertragungskontrolle

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. Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

(Beispiele: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur, Transportsicherung)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter Form |
| <input type="checkbox"/> Verschlüsselung der Datenkommunikation (SAP, Webseiten, E-Mail (Transport)) | <input type="checkbox"/> Geheimhaltungsvereinbarungen mit Mitarbeitern und Dienstleistern abgeschlossen |

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

(Beispiele: Protokollierung, Dokumentenmanagement)

- | | |
|--|--|
| <input type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | <input type="checkbox"/> _____ |

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

a) Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

(Beispiele: Backup-Strategie (online / offline; on-site / off-site), unterbrechungsfreie Stromversorgung (USV), Spiegeln von Festplatten, z.B. RAID-Verfahren, getrennte Aufbewahrung, Virenschutz, Firewall)

- | | |
|--|--|
| <input type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input checked="" type="checkbox"/> Klimaanlage in Serverräumen |
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Backup und Recoverykonzept vorhanden |
| <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen | <input checked="" type="checkbox"/> Getrennte Aufbewahrung der Sicherung |

b) Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c EU DS-GVO)

Maßnahmen zur Gewährleistung der schnellen Wiederherstellbarkeit im Notfall

(Beispiele: Notfallpläne für Rechenzentren, wiederkehrende Notfallübungen, regelmäßige Prüfung der Notfallpläne)

- | | |
|--|--|
| <input type="checkbox"/> Notfallpläne für externes Rechenzentren umgesetzt | <input type="checkbox"/> Wiederkehrende Notfallübungen |
| <input type="checkbox"/> Regelmäßige Prüfung der Notfallpläne | <input type="checkbox"/> _____ |

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

a) Datenschutz-Management

Beschreibung des Datenschutz-Managements

(Beispiele: Datenschutzkoordinatoren, Datenschutzbeauftragter (intern, extern), Rechtsanwälte, Datenschutz-Schulungen, Verpflichtung auf das Datengeheimnis)

- | | |
|---|--|
| <input checked="" type="checkbox"/> Datenschutzkoordinator benannt | <input type="checkbox"/> Datenschutzstrategie/ -konzept |
| <input checked="" type="checkbox"/> Benennung eines Datenschutzbeauftragten | <input type="checkbox"/> Durchführung von Datenschutz-Schulungen |
| <input type="checkbox"/> Verpflichtung auf das Datengeheimnis | <input type="checkbox"/> Rechtsberatung |
| <input type="checkbox"/> Regelmäßige Auditierung der technischen und organisatorischen Maßnahmen durch eine unabhängige Instanz | <input checked="" type="checkbox"/> Dokumentation von Datenschutzvorfällen |

b) Security- und Risikomanagement

Beschreibung von Security- und Risikomanagement Maßnahmen

(Beispiele: Richtlinien, IT-Sicherheits-Schulungen, IT-Sicherheitsrisikomanagement etc.)

- | | |
|--|--|
| <input type="checkbox"/> Erstellung von IT-Richtlinien | <input type="checkbox"/> Regelmäßiger Sicherheitsbericht für das externe Rechenzentrum |
| <input type="checkbox"/> Regelmäßige Ausbildung und Pflichtschulung aller Mitarbeiter zum Umgang mit sensiblen Daten und zur Datensicherheit | <input type="checkbox"/> Penetrationstest |
| <input type="checkbox"/> Code Analysen | <input type="checkbox"/> _____ |

c) Zertifizierungen

Auflistung von Zertifizierungen

- | | |
|---|--------------------------------|
| <input type="checkbox"/> Externes Rechenzentrum ist ISO-27001, ISO-20000 und ISO-9001 zertifiziert. Zusätzlich diverse SAP Zertifizierung | <input type="checkbox"/> _____ |
|---|--------------------------------|

d) Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden

- | | |
|--|---|
| <input checked="" type="checkbox"/> Meldeprozess für Datenschutzverletzungen gegenüber den Betroffenen | <input type="checkbox"/> Überwachung von Sicherheitsvorfällen |
|--|---|

Hinzuziehen von Spezialisten

Meldeprozess für Datenschutzverletzungen gegenüber den Aufsichtsbehörden

e) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU DS-GVO)

Maßnahmen zur Sicherstellung von „Privacy by Design“ und „Privacy by Default“

(Beispiele: Einhaltung der Datenschutzgrundsätze, Einhaltung der Grundprinzipien von Privacy by Design, Verschlüsselung, Festgelegte Löschrufen, Konfigurationsmöglichkeiten für datenschutzfreundliche Voreinstellungen)

Einhaltung der Datenschutzgrundsätze

Einhaltung der Grundprinzipien von Privacy by Design

Festgelegte Löschrufen

Einhaltung von Stand der Technik

Verschlüsselung von Datenkommunikation

Konfigurationsmöglichkeiten für datenschutzfreundliche Voreinstellungen

f) Auftragskontrolle

Maßnahmen im Sinne von Art. 28 EU-DS-GVO, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Artikel 28 DSGVO)

Verpflichtungserklärung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (Artikel 32 Abs.4 DSGVO)

Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Sicherstellung der Vernichtung oder Anonymisierung von Daten nach Beendigung des Auftrags

Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
