Anlage 1: Datensicherheitskonzept

Maßnahmen der data kulturlink ag zur Datenschutzkontrolle gemäß Art. 32 DS-GVO

(Stand 26.3.2018)

1. Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten bei der data kulturlink ag. Alle Mitarbeiter sind zur Einhaltung dieser Richtlinie verpflichtet.

2. Datenschutzbeauftragter

Die data kulturlink ag hat nach Maßgabe der §§ 4f und d BDSG einen betrieblichen Datenschutzbeauftragten (ebDSB) bestellt. Bei Fragen zur zum Datenschutz und dem Datensicherheitskonzept wenden Sie sich bitte an den Datenschutzbeauftragten: Rostenthaler Strasse 38, 10178 Berlin, datenschutz@kulturkurier.de.

3. Grundsätze

Die Datenschutzmaßnahmen der data kulturlink ag haben das Ziel der sicheren Speicherung, der gesicherten Verfügbarkeit der Daten, der Integrität, der Vertraulichkeit, der Nichtverkettbarkeit durch Zweckbestimmung, der Tranzparenz durch Prüffähigkeit sowie der Intervenierbarkeit durch Ankerpunkte.

Sämtliche von data kulturlink ag getroffenen Maßnahmen, insbesondere Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten werden auf einem aktuellen Schutzniveau durchgeführt. Hierzu setzen wir auf geeignete Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Alle Maßnahmen zur Datensicherheit haben auch das Ziel der sicheren und zuverlässigen Bereitstellung der Daten, insbesondere durch die regelmäßige Überprüfung der dauerhaften, hohen Belastbarkeit unserer und der von unseren Unterauftragnehmern im Hosting eingesetzten Systeme.

Wir stellen die Fähigkeit sicher, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Ferner verwenden wir ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Überdies unternehmen der Verantwortliche sowie der Auftragsverarbeiter Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Sämtliche Geschäftsprozesse der data kulturlink ab tragen den Anforderungen der geltenden Vorschriften zum Datenschutz und insb. den Anforderungen der Datenschutz - Grundverordnung Rechnung.

4. Verpflichtung auf das Datengeheimnis

Alle Mitarbeiter der data kulturlink ag sind schriftlich auf diese Richtlinie zur Datensicherheit verpflichtet.

5. Technisch organisatorische Maßnahmen

Der Auftragnehmer bedient sich beim Hosting der Server und allen gespeicherten Daten dem in Anlage 2 bezeichneten Unterauftragnehmer. Sämtliche für den Auftraggeber gespeicherten und verarbeiteten Daten werden ausschließlich auf den beim Unterauftraggeber gemieteten Servern gespeichert. Dies gilt auch für die Backup Systeme.

Die mit dem Unterauftragnehmer abgeschlossene Vereinbarung über die Datenverarbeitung und die Technisch organisatorischen Maßnahmen auf Grundlage des Sicherheitskonzeptes des Unterauftragnehmers sind als Anlage 3 beigefügt.

In den Geschäftsräumen des Auftragnehmers haben nur berechtigte Personen Zugriff auf die Datenverarbeitungssysteme. Es gelten die folgenden technisch organisatorischen Maßnahmen:

Zutrittskontrolle

Der Auftragnehmer sichert dem Auftraggeber zu, dass Unbefugten durch folgende Maßnahmen der Zutritt sowie der Zugang zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet oder gesichert werden:

- Zutritt zu den Büroräumen nur durch oder in Begleitung von berechtigten Personen ·
- Zentrale Zutrittsregelung für Büroräume (biometrische Zugangssperren und Schlüsselkonzept)
- Brandmeldeanlage
- Lagerung von vertraulichen Dokumenten ausschließlich unter Verschluss in abschließbaren, massiven Schränken.
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Der Auftragnehmer sichert zu, dass Unbefugte durch folgende Maßnahmen an der Benutzung der Datenverarbeitungssysteme gehindert werden:

- Passwortschutz: Passwörter mit min. 8 Zeichen inkl. zwei Sonderzeichen. Passwörter werden alle 90 Tage ändert.
- persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Zuordnung von Benutzerrechten: Ein Benutzerstammsatz pro User
- Passwortvergabe Authentifikation mit Benutzername / Passwort

Zugriffskontrolle

Die im Unternehmen getroffenen Maßnahmen der Vertraulichkeit und Integrität gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Darüber hinaus wird sichergestellt, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es werden folgende Maßnahmen getroffen:

- Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- physische Löschung von Datenträgern vor Wiederverwendung
- Passwortschutz: Passwörter mit min. 8 Zeichen inkl. zwei Sonderzeichen. Passwörter werden alle 90 Tage ändert.

Weitergabekontrolle

Die data kulturlink ag versichert hiermit, dass über die gesetzlich vorgesehenen Ausnahmefälle hinaus keinerlei Daten an Dritte weitergegeben werden, es sei denn auf Grundlage einer Weisung des Auftraggebers.

Die folgenden Maßnahmen 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.

- Weitergabe per E-Mail nur über verschlüsselte Emails
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Transportmaterial

Eingabekontrolle

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

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl von Auftragnehmern und Unterauftragnehmer unter Sorgfaltsgesichtspunkten
- Auftragnehmern und Unterauftragnehmer haben Datenschutzbeauftragten bestellt
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer und Unterauftragnehmer getroffenen Sicherheitsmaßnahmen
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Verfügbarkeitskontrolle

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

- Tägliches Backup-Verfahren beim Unterauftragnehmer
- Spiegeln von Festplatten beim Unterauftragnehmer (RAID-Verfahren)
- Notstromversorgung beim Unterauftragnehmer
- Virenschutz / Firewall beim Unterauftragnehmer
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans

Trennungsgebot

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

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)