Technische und organisatorische Maßnahmen

Stand: 01.11.2020

Präambel

Das nachfolgende Dokument dient nur der erläuternden Darstellung gesetzlicher Anforderungen in Bezug auf den Datenschutz. Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus diesem Dokument keine Ansprüche abgeleitet werden. Technische Änderungen und/oder Änderungen in der Organisation, die keinen Einfluss auf die Erfüllung der gesetzlichen Anforderungen der DS-GVO in der jeweils aktuellen Fassung haben, bedürfen keiner gesonderten Information gegenüber dem Vertragspartner.

Bei der k+k information services GmbH, Höhenstr. 16, 70736 Fellbach (nachfolgend „Auftragnehmer“ oder „k+k“) sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1. Zutrittskontrolle

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

Die Büroräume von k+k befinden sich in einem Bürohaus in Fellbach. Es kommt ein elektronisches Schließsystem zum Einsatz, das von k+k verwaltet wird. Nicht befugten Personen ist der Zutritt zu den Räumlichkeiten von k+k nicht gestattet. Sämtliche Personen, die Zutritt zu den Büroräumen erhalten, werden elektronisch erfasst.

Die Anwesenheit von Personen in den Räumlichkeiten von k+k wird über Anwesenheitsaufzeichnungen protokolliert.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Jeder Besucher wird in einem Besucherbuch protokolliert und dann von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die für den SaaS-Betrieb notwendigen Rechenzentren und Serverräume befinden sich nicht in den Räumlichkeiten von k+k.

2. Zugangskontrolle

Durch die Zugangskontrolle wird verhindert, dass die Datenverarbeitungs–systeme der k+k von Unbefugten genutzt werden können. Hält sich die bei Zutritt kontrollierte Person bereits in einem Raum auf, in dem sich die Daten-verarbeitungsanlagen der k+k befinden, wird sichergestellt, dass die betreffende Person diese Datenverarbeitungsanlage nicht benutzen darf. Es ist jederzeit nachvollziehbar, wer wann welches Datenverarbeitungssystem benutzt hat.

Für die Zugangskontrolle sind nachfolgende Maßnahmen von k+k getroffen worden:

2.1. Zugangsberichtigung

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberech-tigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung oder Geschäftsführung gestellt werden.

2.2. Benutzername und Passwörter

Jeder Benutzer von k+k erhält einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort aus Groß-/ Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Passwörter werden alle 90 Tage gewechselt. Die Passworthistorie der einzelnen Nutzer ist hinterlegt. So wird sichergestellt, dass einmal genutzte Passwörter nicht noch einmal verwendet werden können. Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter werden grundsätzlich verschlüsselt gespeichert.

2.3. Anmeldeprotokolle

Sämtliche Anmeldeversuche auf allen IT-System werden protokolliert. Bei 3-maliger Fehleingabe erfolgt in der Regel eine Sperrung des jeweiligen Benutzer-Accounts.

2.4. Zwei-Faktor-Authentifizierung

Eine zusätzliche Zwei-Faktor-Authentifizierung, welche bei der Anmeldung einen weiteren Identitätsnachweis des Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten verlangt, bringt zusätzliche Sicherheit bei der Anmeldung.

2.5. Remote-Zugriffe

Remote-Zugriffe auf die IT-Systeme von k+k erfolgen stets über verschlüsselte Verbindungen.

2.6. Entziehung von Berechtigungen

Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug von Berechtigungen erfolgt i.d.R. sofort muss spätestens binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

3. Zugriffskontrolle

Darunter sind Maßnahmen zu verstehen, 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.

k+k stellt sicher, dass die berechtigte Personen ausschließlich auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung besitzen (need-to-know-Prinzip) und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Zugriff auf personenbezogene Daten wird kontrolliert, indem dieser in Logdateien des Systems manipulationssicher protokolliert wird. Wenn sich eine befugte Person in einem Raum mit einer Datenverarbeitungsanlage befindet und das System benutzt, ist sichergestellt sein, dass sie nur auf die Daten zugreifen kann, für die sie die entsprechende Berechtigung besitzt (Berechtigungskonzept). Dabei ist nachvollziehbar, wer wann auf welche Daten zugegriffen hat.

Berechtigungen für IT-Systeme und Applikationen von k+k werden ausschließlich von Administratoren eingerichtet. Voraussetzung für eine Berechtigung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten. Zusätzlich kann eine Freigabe für einzelne Dateien im Bedarfsfall durch den Administrator vorgenommen werden. Um eine Freigabe einzuräumen, muss ein Antrag durch den Vorgesetzten bzw. den Geschäftsführer vorliegen.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 innerhalb von 24 Stunden gewährleistet. Alle Mitarbeiter bei k+k sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Für die Verarbeitung von personenbezogenen Daten sind die Beschäftigten von k+k verpflichtet nur auf getestete und freigegebene Anwendungssoftware zurückzugreifen. Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Personenbezogene Daten werden auf sicheren DS-GVO konformen Datenservern gespeichert. Das Speichern von Daten auf lokale Datenträger ist nicht vorgesehen. Eine lokale Speicherung von Daten auf einem lokalen Datenträger erfordert die Freigabe durch den Vorgesetzten.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

4. Trennungskontrolle

Alle von k+k für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

5. Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich nur über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Verschlüsselungssysteme im Einsatz.

6. Eingabekontrolle

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

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von k+k im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

7. 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.

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von k+k erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert. Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei im Zusammenhang mit Kundenprojekten untersagt. Beim Ausscheiden der Mitarbeiter werden eventuell bestehende Zugriffsrechte zur Weitergabe von Daten aufgehoben.

Mitarbeiter bei k+k werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

8. Verfügbarkeit und Belastbarkeit

k+k stellt sicher, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Die Verfügbarkeit der Daten wird regelmäßig kontrolliert, d. h. es wird sichergestellt, dass die personenbezogenen Daten zu festgelegten Zeiten im festgelegten Umfang zur Verfügung gestellt werden. Die Verfügbarkeit selbst entspricht dabei den rechtlichen und betrieblichen Erfordernissen, so dass u. a. bei Wartungsfenstern für die Pflege und Wartung der Systeme und Software, diese den laufenden Betrieb nicht negativ beeinflussen.

k+k nutzt für die Speicherung und Verwaltung von personenbezogen Daten, sowie für die Bereitstellung von Servern einen Cloud-Dienstleister und betreibt in den eigenen Räumlichkeiten keine eigenen Server. k+k stellt dabei regelmäßig die Eignung und Sicherheit der zu Verfügung gestellten Dienste sicher und prüft eventuell vorliegende Zertifizierungen.

9. Sicheres Design

Sämtliche Daten werden von k+k verschlüsselt gespeichert, sowohl wenn sie sich auf einem lokalen Datenträger befinden, auf Sicherungsmedien gespeichert werden, oder wenn sie über das Internet übertragen werden.

Personenbezogen Daten liegen stets mehrfach redundant Form in voneinander unabhängigen Datencentern vor, das heißt die Daten liegen gespiegelt und örtlich getrennt vor.

Daten auf den Serversystemen von k+k werden mehrmals täglich inkrementell und täglich vollständig gesichert. Die Sicherungsdaten werden verschlüsselt und in einem virtuell abgetrennten Cloud-Speicher separat gespeichert und verwaltet. Das Einspielen von Backups wird regelmäßig getestet.

Die eingesetzten Rechenzentren sind darauf ausgelegt, Funktionsausfälle zu antizipieren und zu tolerieren und dabei Servicelevel aufrecht zu erhalten. Für das Eintreten eines Funktionsausfalls wird der Datenverkehr von dem vom Ausfall betroffenen Bereich auf einen anderen umgeleitet. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die verbleibenden Standorte aufgeteilt werden kann.

10. Physischer Zugriff

Der Zugang von k+k genutzten Rechenzentren wird regelmäßig durch den Betreiber geprüft. Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.

11. Überwachung und Erkennung

Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.

Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offengehalten wird.

In der Datenebene sind elektronische Einbruchmeldesysteme installiert, die sicherheitsrelevante Ereignisse erkennen und automatisch die zuständigen Mitarbeiter alarmieren. Die Ein- und Ausgänge der Serverräume sind durch Geräte gesichert, an denen Personal Multi-Faktor-Authentifizierungsverfahren durchlaufen müssen, bevor sie den Raum betreten oder verlassen können. Diese Geräte lösen einen Alarm aus, wenn die Tür ohne Autorisierung aufgebrochen oder offengehalten wird. Die Türalarmsysteme sind so konfiguriert, dass sie erkennen, wenn jemand eine Datenebene ohne Multi-Faktor-Autorisierung betritt oder verlässt. In diesem Fall wird umgehend ein Alarm ausgelöst.

12. Gerätemanagement

Medienspeichergeräte, auf denen personenbezogene gespeichert sind, werden vom Betreiber der Datencenter als kritisch eingestuft und deshalb über ihren gesamten Lebenszyklus als höchst dringlich behandelt. Der Betreiber des Datencenters hat bestehende Normen, wie die Geräte installiert, betrieben und irgendwann zerstört werden, wenn sie nicht mehr verwendet werden. Wenn ein Speichergerät das Ende seines Lebenszyklus erreicht hat, wird es gemäß zertifizierten Techniken stillgelegt. Medien, auf denen Kundendaten gespeichert wurden, werden erst nach erfolgter Stilllegung aus der Hand gegeben.

13. Betriebliche Support-Systeme

Die elektrischen Anlagen der eingesetzten Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können. Dabei ist sichergestellt, dass die Rechenzentren mit einer Notstromversorgung ausgestattet sind, damit im Fall eines Stromausfalls der Betrieb von kritischen Lasten der Anlage gewährleistet ist.

Die genutzten Rechenzentren verfügen über Klimaanlagen zur Kontrolle der Betriebstemperatur für Server und andere Hardware, um eine Überhitzung zu vermeiden und das Risiko von Serviceausfällen zu verringern. Temperatur und Luftfeuchtigkeit werden in angemessener Weise vom Personal und den technischen Systemen überwacht und geregelt.

Die Rechenzentren sind mit automatischen Geräten zur Branderkennung und -bekämpfung ausgestattet. Die Branderkennungssysteme setzen Rauchsensoren in vernetzten, mechanischen und Infrastrukturbereichen ein. Diese Bereiche sind darüber hinaus durch Brandbekämpfungssysteme geschützt.

Um Wasserlecks erkennen zu können, sind die Rechenzentren mit Wasser-erkennungssensoren ausgestattet. Wenn Wasser entdeckt wird, wird dieses entfernt, um zusätzliche Wasserschäden zu vermeiden.

14. Governance und Risiko

Die von k+k eingesetzten Rechenzentren sind darauf ausgelegt, Funktionsausfälle zu antizipieren und zu tolerieren und dabei Servicelevel aufrecht zu erhalten. Für das Eintreten eines Funktionsausfalls wird der Datenverkehr von dem vom Ausfall betroffenen Bereich auf einen anderen umgeleitet. Für wichtige Anwendungen gilt ein N+1-Standard. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die verbleibenden Standorte aufgeteilt werden kann.

Es werden zudem regelmäßig Bedrohungs- und Schwachstellenprüfungen der Rechenzentren durch den Betreiber durchgeführt. Die fortlaufende Bewertung und Abwehr von potenziellen Schwachstellen erfolgt über die Risikobewertungs-aktivitäten der Rechenzentren. Dabei werden auch regionale behördliche und Umweltrisiken berücksichtigt.

Ein Betriebskontinuitätsplan des Betreibers umfasst Maßnahmen zur Vermeidung und Verringerung von Störungen durch Umwelteinflüsse. Der Plan enthält betrieb-liche Details zu den Maßnahmen, die vor, während und nach einem entsprechen-den Ereignis ergriffen werden. Der Betriebskontinuitätsplan wird durch Tests gestützt, die auch Simulationen verschiedener Szenarios umfassen.

15. Auftragskontrolle

Im Rahmen der Auftragskontrolle wird gewährleistet, dass personenbezogenen Daten, die im Auftrag verarbeitet werden, nur auf Grundlage des Vertrages entsprechend den Weisungen des Auftraggebers (Verantwortlichen) verarbeitet werden.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbei-tungsvertrag nach zuvor durchgeführtem Audit durch den Datenschutz-beauftragten von k+k abgeschlossen.

16. Datenschutzfreundliche Voreinstellungen

Bei k+k wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirm-masken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder teil-weise deaktiviert werden.

Die Software von k+k unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen für Daten oder Funktionalitäten können flexibel und granular gesetzt werden.

17. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei k+k ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.