# Technische und organisatorische Maßnahmen

Gültig ab 01.09.2020

a) Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

b) Konkretisierung der Einzelmaßnahmen

Der Auftragnehmer setzt die Anforderungen wie folgt in seinem Einflussbereich in Bezug auf diese Vereinbarung um. Darüber hinaus ist im Rahmen der besonderen Vertragskonstellation zwischen dem Cloud-Dienste Anbieter Microsoft, dem IT-Dienstleister als Auftragnehmer und dem Auftraggeber hinsichtlich der Konkretisierung der Einzelmaßnahmen auch auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen.

## 1. Zutrittskontrolle

a) Mit dem Begriff „Zutritt“ ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT-Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und die Netzverkabelungen befinden und verlegt sind, gehören hierzu. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden (können), zu verwehren. Der Auftragnehmer muss deshalb dafür Sorge tragen, dass Unbefugte Räume, in denen Daten vom Auftraggeber verarbeitet oder gespeichert werden, nicht betreten können und keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (Monitore, Drucker, etc.) erlangen können, auf denen diese Daten verarbeitet oder ausgegeben werden.

b) <u>Umsetzung der Zutrittskontrolle bei Celes Systems Büroräume</u>

Der Auftragnehmer hat die folgenden Maßnahmen zur Zutrittskontrolle umgesetzt:

Die Eingangstüren des Gebäudes sind mit folgender Schließanlage versehen:

☒ Manuelle Schließanlage ☐ Chipkarten Schließanlage

☒ Es besteht ein gesondertes Zutrittskonzept für Serverräume

c) <u>Umsetzung der Zutrittskontrolle bei Celes Systems Rechenzentren</u>

Der Auftragnehmer hat die folgenden Maßnahmen zur Zutrittskontrolle umgesetzt:

Die Eingangstüren des Gebäudes sind mit folgender Schließanlage versehen:

☒ Manuelle Schließanlage (Frankfurt)

☒ Chipkarten Schließanlage (Frankfurt)

☒ Biometrische Schließanlage (München)

☒ Die Nutzung der Schließanlage wird dokumentiert.

☒ Der Zutritt und Aufenthalt von Besuchern erfolgt nur in Begleitung von Firmenpersonal oder Personal des Rechenzentrumsbetreibers.

☒ Der Entzug von Gebäudezutrittsberechtigungen ist geregelt und dokumentiert.

☒ Es besteht ein gesondertes Zutrittskonzept für Serverräume

d) Umsetzung der Zutrittskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Zutrittskontrolle zu Microsoft Systemen sind in den Online Services Terms beschrieben.

## 2. Zugangskontrolle

a) Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV-Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden. Unbefugte dürfen keinen Zugang zu den Datenverarbeitungssystemen des Auftragnehmers erlangen können. Daher muss der Auftragnehmer die mit der Erfüllung der Leistungen des Auftrags beauftragten Personen mit einer sicheren Benutzeridentifikation versehen. Desweitern ist auf die spezifischen Sicherheitsmaßnahmen hinsichtlich der Zugangskontrollen zu den Microsoft Rechenzentren auf die Bestimmungen in den Online Services Terms zu verweisen.

b) Umsetzung der Zugangskontrolle bei Celes Systems GmbH

Der Auftragnehmer hat die folgenden Maßnahmen zur Zugangskontrolle umgesetzt:

☒ Das Firmennetzwerk ist durch eine Firewall geschützt

☒ Die Daten des Auftraggebers werden innerhalb des Firmennetzwerkes separiert

Die Mitarbeiter des Auftragnehmers müssen folgende Passwortvorgaben erfüllen:

☒ Individuelle Passwörter für verschiedene Systeme (keine Sammelpasswörter)

☒ Die Passwörter haben eine Mindestlänge/Komplexität, wenn zutreffend Anzahl der Zeichen:

8

☒ Die Passwörter müssen regelmäßig gewechselt werden, wenn zutreffend Intervall angeben:

60 Tage

☐ Der Zugang zum System wird gesperrt bei der fehlerhaften Eingabe des Passwortes, bitte Anzahl der Fehlversuche und Dauer der Sperrung angeben:

_____

An den folgenden Übergängen zum Firmennetzwerk werden Virenscanner eingesetzt:

☒ E-Mail Account ☐ FTP ☒ Web

☐ Mitarbeiter haben keine lokale Administrationsrechte

c) Umsetzung der Zugangskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Zugangskontrolle zu Microsoft Systemen sind in den Online Services Terms beschrieben.

## 3. Zugriffskontrolle

a) Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können. Es dafür zu sorgen, 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.

b) Umsetzung der Zugriffskontrolle bei Celes Systems GmbH

Der Auftragnehmer hat die folgenden Maßnahmen zur Zugriffskontrolle umgesetzt:

☒ Ein Berechtigungskonzept ist vorhanden

☒ Die Anzahl der Administratoren mit Berechtigung ist auf ein Mindestmaß beschränkt

c) Umsetzung der Zugriffskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Zugriffskontrolle zu den Microsoft Systemen sind in den Online Services Terms beschrieben.

## 4. Weitergabekontrolle

a) Der Auftragnehmer muss verhindern, dass personenbezogene Daten vom Auftraggeber 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

b) Umsetzung der Weitergabekontrolle

Im Rahmen der Nutzung von Microsoft Online Diensten, liegt die Umsetzung der Weitergabekontrolle bei Microsoft. Microsoft setzt im Rahmen der Online Dienste bei der Datenübertragung über das Internet

auf TLS Verschlüsselung. Der Auftraggeber hat zudem jederzeit die Möglichkeit weitere von Microsoft zur Verfügung gestellte Sicherheitstools als zusätzlichen Service auszuwählen und zu aktivieren.

## 5. Eingabekontrolle

a) Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es müssen daher für derartige Maßnahmen entsprechende Protokollierungssysteme vorhanden sein.

b) Umsetzung der Eingabekontrolle

Im Rahmen der Nutzung von Microsoft Online Diensten, liegt die Umsetzung der Eingabekontrolle bei Microsoft. Microsoft bietet seinen Nutzern über das Trust Center einen Protokolldienst an. Mit diesem können Zugriffsberichte ausgeführt werden. An Hand dieser Berichte kann eine Eingabekontrolle nachgewiesen werden.

## 6. Auftragskontrolle

a) Die Kategorie Auftragskontrolle stellt sicher, dass die Daten, die im Auftrag des Kunden verarbeitet werden, auch nur dementsprechend verarbeitet werden können und keine fremden oder ungewollten Verarbeitungen stattfinden Der Auftragnehmer muss gewährleisten, dass personenbezogene Daten vom Auftraggeber nur gemäß deren Weisungen verarbeitet werden. Beschäftigt der Partner einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.

b) Umsetzung der Auftragskontrolle bei der Celes Systems GmbH

Der Auftragnehmer hat die folgenden Maßnahmen zur Auftragskontrolle umgesetzt:

☒ Die Mitarbeiter werden schriftlich auf das Datengeheimnis gem. §5 BDSG verpflichtet

☒ Die Mitarbeiter erhalten Schulungen zum Datenschutz

c) Umsetzung der Auftragskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Auftragskontrolle sind in den Online Services Terms beschrieben.

## 7. Verfügbarkeitskontrolle

a) Der Auftragnehmer muss dafür sorgen, dass personenbezogene Daten vom Auftraggeber gegen zufällige Zerstörung oder Verlust geschützt sind.

b) Umsetzung der Verfügbarkeitskontrolle bei der Celes Systems GmbH

Der Auftragnehmer hat die folgenden Maßnahmen zur Verfügbarkeitskontrolle umgesetzt:

Häufigkeit der Datensicherungsmaßnahmen:

☒ täglich ☐ monatlich ☐ jährlich

Aufbewahrungsort von Sicherungsdatenträgern:

☐ Safe ☒ externe Auslagerung

c) Umsetzung der Verfügbarkeitskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Verfügbarkeitskontrolle sind in den Online Services Terms beschrieben.

## 8. Trennungsgebot

a) Es ist dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten muss so gestaltet sein, dass eine „Vermischung" mit Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers und auch unbefugte Zugriffe Dritter (auch versehentlich) unmöglich sind. Sollten Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers von behördlichen Zugriffen bzw. Beschlagnahme betroffen sein, muss gewährleistet sein, dass die Daten vom Auftraggeber davon unberührt bleiben. Die Daten dürfen nicht zu Testzwecken herangezogen werden, welche nicht Bestandteil der Leistungen des Hauptvertrages sind.

b) Umsetzung des Trennungsgebotes bei der Celes Systems GmbH

Der Auftragnehmer hat die folgenden Maßnahmen zum Trennungsgebot umgesetzt:

☒ Daten des Auftraggebers werden in einem eigenen Mandat vorgehalten

☒ Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte mit einzubringen

c) Umsetzung des Trennungsgebotes bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich des Trennungsgebotes sind in den Online Services Terms beschrieben.

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 dem Auftraggeber unmittelbar zu melden.