

8. Rechte und Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist der Auftraggeber verantwortlich. Der Auftragnehmer dokumentiert die Erteilung aller Aufträge, Teilaufträge oder Weisungen. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren sowie Nachweise über die Einhaltung der in diesem Vertrag niedergelegten Pflichten anzufordern. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer – soweit erforderlich – Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen.

9. Fernmeldegeheimnis

Der Auftragnehmer sichert die Wahrung des Fernmeldegeheimnisses entsprechend § 88 TKG zu. Dazu muss der Auftragnehmer alle Personen, die auf Daten des Auftraggebers durch Mittel der Telekommunikation wie E-Mail, Telefon oder Telefax zugreifen können, auf die Wahrung des Fernmeldegeheimnisses verpflichten und entsprechend belehren.

10. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelungen. Eine eventuell zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung.

11. Beendigung

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis nach Wahl des Auftraggebers stehen, entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Löschung oder Sperrung ist in geeigneter Weise zu dokumentieren. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe, Löschung oder Sperrung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen.

Anlage 1

Technisch Organisatorische Maßnahmen

1. Leitbild und Zielsetzung

Wir streben eine langfristige Beziehung zu unseren Mitarbeitern und eine durchgängig hohe Zufriedenheit unserer Kunden an. Dabei stellen wir insbesondere die Gestaltung der individuellen Beziehung zu unseren Kunden in den Mittelpunkt und richten alle weiteren Unternehmensziele daran aus. Ein wichtiger Teil dieser Beziehungen basiert auf Vertrauen. Daher treten wir vollumfänglich für den Schutz der Privatsphäre und des Rechts auf Datenschutz ein. Unser Ziel ist es, Mitarbeitern, Kunden und Besuchern einen sicheren, risikolosen Service anzubieten. Um sicherzustellen, dass personenbezogene Daten nur in Übereinstimmung mit den gesetzlichen Grundlagen erfolgt, richten wir unsere Prozesse und technische Gestaltung an den Gewährleistungszielen der Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes und der weiteren relevanten Gesetze aus. Insbesondere sollen nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind und einfache Ausübung der Betroffenenrechte sichergestellt werden. Die folgenden TOMs richten sich nach den Gewährleistungszielen des Art. 32 sowie der Regelung des Art. 25 der Datenschutzgrundverordnung.

2. Maßnahmen

2.1. Grundlegende Schutzmaßnahmen Wir trennen nach Möglichkeit und an den erforderlichen Stellen personenbezogene Daten von den verarbeiteten Daten, so dass eine Verknüpfung der verarbeiteten Daten mit einer identifizierten oder identifizierbaren Person ohne zusätzliche Informationen, die gesondert und sicher aufbewahrt werden, nicht möglich ist. Dies gilt insbesondere, wenn Daten im Rahmen von Forschungsvorhaben verarbeitet werden. Zudem verschlüsseln wir insbesondere zur Übertragung vorgesehene personenbezogene Daten mit einem dem Stand der Technik entsprechenden Verfahren.

2.2. Zutrittskontrolle Die eingerichteten Maßnahmen zur Zugriffskontrolle gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird. Wir schützen unsere für die Verarbeitung von personenbezogenen Daten kritischen Bereiche durch angemessene Zutrittskontrollsysteme wie Klingelanlagen, Videoüberwachung von kritischen Bereichen, automatische Zugangskontrollsysteme und manuelle Schließsysteme. Zudem werden für besonders schutzwürdige Bereiche zusätzliche Sicherheitsmaßnahmen ergriffen. Es handelt sich insbesondere um Alarmanlagen, Lichtschranken/Bewegungsmelder, Einsatz von Wachpersonal und eine Protokollierung der Besucher. Zutrittsrechte für berechtigte Personen werden gemäß festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen.

2.3. Zugangskontrolle Zugang zu Datenverarbeitungssystemen erhalten nur authentifizierte Benutzer aufgrund eines rollenbezogenen Berechtigungskonzepts unter Verwendung von folgenden Maßnahmen: individualisierte Passwortvergabe und Benutzerprofilen sowie regelmäßig aktualisierte Antiviren- und Spam-Filter im Netzwerk und auf den einzelnen PCs. Zudem werden für besonders schutzwürdige Bereiche zusätzliche Sicherheitsmaßnahmen ergriffen. Es handelt sich insbesondere um den Einsatz von Hard- und Softwarefirewalls und den Einsatz von VPN Technologie.

2.4. Zugriffskontrolle Die eingerichteten Maßnahmen zur Zugriffskontrolle 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. Der Zugriff auf personenbezogene Daten wird auf der Grundlage einer projektbezogenen Berechtigung gewährt. Es ist ein Benutzerverwaltungssystem eingerichtet, welches den Zu- und Abgang von Nutzern mit ihren jeweiligen Berechtigungen unter der Steuerung von Systemadministratoren abbildet. Die Vergabe von Passwörtern basiert auf einer Passwortrichtlinie, die die erforderliche Länge und Wechselintervalle regelt. Die Anzahl der Systemadministratoren wurde auf das „Notwendigste“ beschränkt. Datenträger werden datenschutzgerecht entsorgt. Zudem werden für besonders schutzwürdige Bereiche zusätzliche Sicherheitsmaßnahmen ergriffen. Es handelt sich insbesondere um die Protokollierung von Zugriffen auf Anwendungen, besonders bei der Eingabe, Änderung und Löschung von Daten.

2.5. Datenübertragungskontrolle Wir sichern die elektronischen Kommunikationswege durch Einrichtung geschlossener Netzwerke und Verfahren zur Datenverschlüsselung ab. Dadurch stellen wir sicher, 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. Sofern ein physischer Datenträgertransport erfolgt, werden auf der Basis einer Risikoabschätzung im Einzelfall Maßnahmen ergriffen, welche den unbefugten Datenzugriff oder den logischen Verlust verhindern. Werden Daten elektronisch übermittelt, geschieht dies unter Nutzung von Standleistung beziehungsweise VPN Technologie. Allgemein wird eine verschlüsselte Übertragung nach Möglichkeit bevorzugt.

2.6. Eingabekontrolle Zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, findet eine weitgehende Eingabekontrolle statt. In diesem Zusammenhang ist die Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen sichergestellt. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis eines projektbezogenen Berechtigungskonzepts. Zudem werden für besonders schutzwürdige Bereiche zusätzliche Sicherheitsmaßnahmen ergriffen. Es handelt sich insbesondere um die Protokollierung von Zugriffen auf Anwendungen, besonders bei der Eingabe, Änderung und Löschung von Daten.

2.7. Trennungskontrolle Durch eine logische und physikalische Trennung der Daten gewährleisten wir, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Verwendete Test- und Live-Systeme sind vollständig getrennt. Die relevanten Anwendungen zur Speicherung von Daten sind mandantenfähig. Sie basieren zudem auf festgelegten Datenbankrechten und einem Berechtigungskonzept auf Grundlage eines Need-to-Know-Prinzips.

2.8. Verfügbarkeitskontrolle Wir ergreifen Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen umfassen in erster Linie die direkte Sicherung der Serveranlagen gegen die gegebenen Risiken. Auf der technischen Seite handelt es sich insbesondere um: Feuer- und Rauchmeldeanlagen, unterbrechungsfreie Stromversorgung, Geräte zur Überwachung der Temperatur und Feuchtigkeit, redundante Klimaanlage, Schutzsteckdosen, Feuerlöschgeräte sowie in kritischen Bereichen durch automatisierte Löschanlagen und unterbrechungsfreie Stromversorgung. Zur Gewährleistung der Verfügbarkeit werden diese technischen Maßnahmen durch organisatorische Maßnahmen ergänzt. Zudem werden für besonders schutzwürdige Bereiche zusätzliche Sicherheitsmaßnahmen ergriffen. Es handelt sich insbesondere um Alarmmeldungen bei unberechtigtem Zutritt zu Serverräumen, Erstellung eines Notfallplans und die Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort. Des Weiteren be-

finden sich Serverräume grundsätzlich nicht unter sanitären Anlagen.

2.9. Incident-Response-Management Im Fall von Datenschutzpannen besteht ein Prozess zur Meldung auch im Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde, welcher die Einbeziehung der betroffenen Abteilung und der/des Datenschutzbeauftragte/n umfasst. Der Prozess umfasst ebenso die Bestimmung der Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen unter Einbeziehung eines Data Breach Management Teams.

2.10. Kontrolle der Auftragsverarbeiter Sofern Auftragsverarbeiter eingesetzt werden, ergreifen wir Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. In diesem Zusammenhang erfolgt eine sorgfältige Auswahl des Auftragnehmers in Bezug auf Datenschutz und Datensicherheit und die Sichtung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation. Insbesondere achten wir darauf, dass in der Vereinbarung mit dem Auftragsverarbeiter eine Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis, eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei vorliegender Bestellpflicht, eine Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer, Regelungen zum Einsatz weiterer Subunternehmer, die Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags und eine regelmäßige Überprüfung des Auftragnehmers und seines Schutzniveaus enthalten sind.

3. Datenschutzmanagementsystem

Wir verfügen über eine Kontrollmöglichkeit auf der Grundlage eines risikomanagementbasierten Ansatzes zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung. Damit wird der Schutz der relevanten Informationen, Anwendungen (einschließlich Qualitäts- und Sicherheits-Testmethoden), Betriebsumgebungen (z.B. durch Netzwerküberwachung gegen schädliche Einwirkungen) sowie der technischen Umsetzung von Schutzkonzepten (z.B. mittels Schwachstellenanalysen) gewährleistet. Durch das systematische Erfassen und Beseitigen von Schwachstellen werden damit die Schutzmaßnahmen kontinuierlich hinterfragt und verbessert. Ergänzt wird dieser Prozess durch die risikobasierte Schwachstellenanalyse im Rahmen der ISO27001 Zertifizierung. Darüber hinaus wird ein Datenschutzmanagementsystem auch durch eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter im Betrieb aktiv gelebt. Diese Maßnahmen werden durch die Bestellung des Datenschutzbeauftragten, die Schulung der Mitarbeiter und die Verpflichtung auf Vertraulichkeit sowie das Datengeheimnis festgelegt. Anlassbezogen kommen wir unseren Informationspflichten gemäß Art. 13 und 1 DSGVO, dem Widerrufsrecht der Betroffenen, der Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung und der Bearbeitung von Auskunftsanfragen seitens Betroffener nach.

Anlage 2

Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten Leistungen von Unterauftragnehmer in Anspruch. In nachstehender Auflistung finden Sie alle Unterauftragnehmer, deren Dienstleistung in technischer Hinsicht in Anspruch genommen wird. Zur Leistungserfüllung werden nicht notwendigerweise die Leistungen aller Unterauftragnehmer benötigt.

Unternehmen, Rechtsform, Anschrift	Sitz des Unternehmens	Ggf. Feststellung eines angemessenen Schutzniveaus	Kurzbeschreibung der übernommenen Aufgaben
3M Services GmbH Ahrensburger Straße 8 30659 Hannover	Deutschland	Abschluss einer AVV	Umsetzung technische Überwachung
Telemarketing Bleines Goebenstr. 25 66117 Saarbrücken	Deutschland	Abschluss einer AVV	Callcenter
DiaLogika Gesellschaft für angewandte Informatik mbH Albertstraße – Pascalschacht 1 66125 Saarbrücken	Deutschland	Abschluss einer AVV	Abrechnungssystem
DoS-COM GmbH Am Birchelberg 5 66271 Kleinblittersdorf	Deutschland	Abschluss einer AVV	Protokollierung der Zugänge zu den Gebäuden/Räumlichkeiten
heXoNet GmbH Talstr. 27 66424 Homburg	Deutschland	Abschluss einer AVV	Ankauf Domains und SSL-Zertifikate
Key-Systems GmbH Im Oberen Werk 1 66386 St. Ingbert	Deutschland	Abschluss einer AVV	Ankauf Domains und SSL-Zertifikate
nexnet GmbH Linkstr. 2 10785 Berlin	Deutschland	Abschluss einer AVV	Abrechnung Mehrwertdienste
Seloca GmbH Barkauer Str. 121 24145 Kiel	Deutschland	Abschluss einer AVV	Fritzbox Refurbishment und Austausch
T&S Computech GmbH Platherstr. 3a 30175 Hannover	Deutschland	Abschluss einer AVV	Support Davev
XPRON Systems GmbH Carl-Schurz-Straße 2 41460 Neuss	Deutschland	Abschluss einer AVV	Callcenter
Eviso Germany GmbH, Business Partner of M7 Group SA Brüsseler Straße 89 – 93 D-50672 Köln	Deutschland	Abschluss einer AVV	Bereitschaftsdienst SMS, TV
CM Telecom Germany GmbH Office Frankfurt Mainfrankenpark 53 97337 Dettelbach	Deutschland	Abschluss einer AVV	Mitteilungen z. B per SMS