**Beschreibung der technischen und organisatorischen im Serverstandort des Auftragnehmers gemäß Artikel 32 DSGVO**

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die Maßnahmen müssen im Interesse beider Parteien so konkret wie möglich beschrieben werden! Sie sind Maßstab für Kontrollen durch den Auftraggeber und auch für die Frage entscheidend, ob möglicherweise ein Pflichtverstoß vorliegt. In dieser Anlage wird ganz maßgeblich festgelegt, was der Auftragnehmer zu leisten und nachzuweisen hat und was nicht. Unklare oder interpretationsfähige Umschreibungen sind dringend zu vermeiden!

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

1. Organisation der Informationssicherheit
2. Personalsicherheit
3. Verwaltung der Werte
4. Zugangssteuerung
5. Kryptographie
6. Physische und umgebungsbezogene Sicherheit
7. Betriebssicherheit
8. Kommunikationssicherheit
9. Anschaffung, Entwicklung und Instandhaltung von Systemen
10. Lieferantenbeziehungen
11. Handhabung von Informationssicherheitsvorfällen
12. Informationssicherheitsaspekte beim Business Continuity Management
13. Compliance

**Bisher (BDSG) war dies ausreichend:**

1. **Vertraulichkeit**

Maßnahmen, die verhindern, dass Unbefugte personenbezogene Daten zur Kenntnis nehmen können.

* 1. **Zutrittskontrolle**

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Folgende Maßnahmen sind beim Auftragnehmer umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Absicherung von Gebäudeschächten | ☒ | Protokollierung der Besucher |
| ☒ | Alarmanlage | ☒ | Schließsystem mit Codesperre |
| ☒ | Automatisches Zutrittskontrollsystem | ☒ | Schlüsselregelung (Schlüsselliste) |
| ☒ | Biometrische Zutrittskontrollen | ☒ | Sicherheitstüren und -schlösser |
| ☒ | Chipkarten-/Transponder-Schließsystem | ☒ | Sorgfältige Auswahl von Reinigungspersonal |
| ☒ | Einbruchmeldeanlage | ☒ | Sorgfältige Auswahl von Wachpersonal |
| ☒ | Einsatz von Wachpersonal | ☒ | Tragepflicht von Berechtigungsausweisen |
| ☒ | Lichtschranken / Bewegungsmelder | ☒ | Unterteilung in verschiedene Sicherheitszonen |
| ☒ | Manuelles Schließsystem | ☒ | Videoüberwachung der Zugänge |
| ☒ | Personenkontrolle beim Pförtner / Empfang | ☒ | Zutrittsberechtigungen funktions- und rollenbasiert |
| ☒ | sonstiges: Die markierten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf im Rahmen des mehrstufigen Sicherheitszonenkonzeptes des Auftragnehmers zum Einsatz. Die Überwachung des Geländes/Gebäudes erfolgt außerhalb der Geschäftszeiten sowie an Wochenenden und Feiertagen durch einen externen Wachdienst.  |

* 1. **Zugangskontrolle**

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | 2-Faktor-Authentifizierung | ☒ | Passwortregelung (Mindestlänge, Komplexität, Gültigkeitsdauer, Sperrung/Löschung u.a.) |
| ☒ | Authentifikation mit Benutzername / Passwort | ☒ | Schlüsselregelung (Schlüsselausgabe etc.) |
| ☐ | ~~Authentifikation mit biometrischen Verfahren~~ | ☒ | Sichere Aufbewahrung von Datenträgern (Sicherungsbänder, Festplatten etc.) |
| ☒ | Einsatz eines Aktenvernichters | ☐ | ~~Sorgfältige Auswahl von Transportpersonal und -fahrzeugen~~ |
| ☒ | Einsatz von Anti-Viren-Software | ☒ | Vernichtung von Datenträgern durch dafür zertifizierte Entsorgungsfachbetriebe |
| ☒ | Einsatz einer Hardware-Firewall | ☒ | Vernichtung von Papierdokumenten durch dafür zertifizierte Entsorgungsfachbetriebe |
| ☐ | ~~Einsatz eines Identity Management Systems~~ | ☒ | Verschlüsselung auf Verzeichnis- und Dateiebene |
| ☒ | Einsatz einer Software-Firewall | ☒ | Verschlüsselung von Datenträgern in Laptops / Notebooks |
| ☒ | Einsatz verschließbarer Entsorgungsbehälter für Papier, Akten und Datenträger | ☐ | ~~Verschlüsselung von mobilen Datenträgern (USB-Sticks, CD/DVD etc.)~~ |
| ☒ | Einsatz von VPN-Technologie\* | ☒ | Verschlüsselung von Smartphone Inhalten |
| ☒ | Erstellen von Benutzerprofilen | ☐ | ~~Verwendung sicherer Transportbehälter /-verpackungen beim physischen Transport~~ |
| ☒ | Netzwerk- und Netzwerkzonenkonzept | ☒ | Zuordnung von Benutzerprofilen zu IT-Systemen |
| ☐ | ~~Notfallmanagement für Auftraggeber (u.a. Mehrschichtbetrieb, Rufbereitschaft, Stellvertreterregelung)~~ | ☒ | Zuweisung von Benutzerrechten erfolgt funktions- und rollenbasiert |
| ☒ | sonstiges: Die markierten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf im Rahmen des mehrstufigen Sicherheitszonenkonzeptes des Auftragnehmers zum Einsatz. |

* 1. **Zugriffskontrolle**

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.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Anzahl der Administratoren auf ein Minimum begrenzt | ☒ | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten |
| ☒ | Funktions- und rollenbasiertes Berechtigungskonzept | ☒ | Verwaltung der Zugriffsberechtigungen unter Beachtung der Funktionstrennung und des 4-Augenprinzips |
| ☒ | Protokollierung der Vernichtung von Papier, Akten und Datenträgern |  |  |
| ☒ | sonstiges:  |

* 1. **Weitergabekontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | ☒ | Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis gem. § 88 TKG |
| ☒ | E-Mail-Verschlüsselung | ☒ | Verpflichtung der Mitarbeiter auf das Sozialgeheimnis gem. § 35 SGB I |
| ☒ | Einrichtungen von Standleitungen bzw. VPN-Tunneln\* | ☒ | Verpflichtung der Mitarbeiter auf das Verbot des Verrats von Geschäfts- und Betriebsgeheimnissen gem. §§ 17 ff. UWG |
| ☒ | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen\* | ☒ | Verpflichtung der Mitarbeiter auf Zweckbindung und Geheimhaltungspflicht gem. § 78 Abs. 1 SGB X |
| ☒ | Verpflichtung der Mitarbeiter auf das Datengeheimnis gem. § 5 BDSG | ☒ | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form\* |
| ☒ | sonstiges: Die Weitergabe von Daten des Auftraggebers erfolgt nur in Abstimmung mit dem Auftraggeber an die vom ihm vorgegeben Empfänger. Alle Mitarbeiter des Auftragnehmers sind zur Wahrung der Verschwiegenheit sowie des Datengeheimnisses als Bestandteil ihres Arbeitsvertrages mit dem Auftragnehmer verpflichtet und über die rechtlichen Konsequenzen im Fall der Zuwiderhandlung schriftlich belehrt.  |

1. **Integrität**

Maßnahmen, die gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

* 1. **Eingabekontrolle**

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

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind | ☒ | Protokollierung der Eingabe, Änderung und Löschung von Daten |
| ☒ | Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. | ☒ | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
| ☒ | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |  |  |
| ☒ | sonstiges: Die Mitarbeiter des Auftragnehmers erstellen, ändern oder löschen von Daten bzw. Datensätze des Auftraggebers nur auf individuelle, schriftliche Weisung im Rahmen des Incident und Change Managements sinngemäß ISO/IEC 20000-1:2011. Dabei werden sowohl die Freigabe des Auftraggebers als auch die vorgenommenen Änderungen dokumentiert. Eine Übersicht der vorgenommenen Änderungen ist in den monatlichen Berichten an den Auftraggeber enthalten. |

* 1. **Verfügbarkeitskontrolle**

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

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | ☐ | ~~Notfallhandbuch~~ |
| ☒ | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | ☐ | ~~Notfallkonzept (BCM)~~ |
| ☒ | Feuer- und Rauchmeldeanlagen | ☐ | ~~Notfallplan~~ |
| ☒ | Feuerlöschanlagen in Serverräumen | ☒ | Regelungen zur Verfügbarkeit und Zuverlässigkeit der vom Auftragnehmer erbachten Leistung\* |
| ☒ | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | ☒ | Überspannungsschutzkonzept in Serverräumen |
| ☒ | Klimatisierte Serverräume | ☒ | Maßnahmen gegen Wassereinbruch in Serverräume |
| ☒ | Konzept zur Sicherung und Wiederherstellung von Daten (Backup, Restore, Recovery) durch den Auftragnehmer\* | ☒ | Testen von Datenwiederherstellung\* |
| ☒ | Konzept zur Archivierung von Daten durch den Auftragnehmer\* | ☒ | Unterbrechungsfreie Stromversorgung (USV) |
| ☒ | sonstiges: Einzelheiten zu der zwischen Auftraggeber und Auftragnehmer vereinbarten Verfügbarkeit sowie den Backup-, Restore- und Recovery-Maßnahmen sind im zugrundeliegenden Dienstleistungsvertrag beschrieben. Dies gilt auch für die begleitenden, mit \* gekennzeichneten Maßnahmen. |

* 1. **Auftragskontrolle**

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

Folgende Maßnahmen werden zusätzlich zu den vorgenannten Kontrollen vom Auftraggeber und vom Auftragnehmer umgesetzt:

|  |  |
| --- | --- |
| *Maßnahmen, die die Auftragsdatenverarbeitung durch den Auftragnehmer regulieren:*: | *Maßnahmen, die eine mögliche Auftragsdatenverarbeitung durch Unterauftragnehmer des Auftragnehmers regulieren:* |
| ☐ | Auswahl des Auftragnehmers durch den Auftraggeber unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | ☐ | ~~Auswahl des Unterauftragnehmers durch den Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)~~ |
| ☐ | Prüfung des Auftraggebers auf Bestellung eines Datenschutzbeauftragten beim Auftragnehmer | ☐ | ~~Prüfung des Auftragnehmers auf Bestellung eines Datenschutzbeauftragten beim Unterauftragnehmer~~ |
| ☐ | Prüfung der Dokumentation und der beim Auftragnehmer getroffenen Sicherheits­maßnahmen durch den Auftraggeber vor Beginn der Datenverarbeitung | ☐ | ~~Prüfung der Dokumentation und der beim Unterauftragnehmer getroffenen Sicherheits­maßnahmen durch den Auftragnehmer vor Beginn der Datenverarbeitung~~ |
| ☐ | Schriftliche Weisungen des Auftraggebers an den Auftragnehmer nach § 11 Abs. 2 BDSG (z.B. durch Vertrag der Datenverarbeitung im Auftrag) | ☐ | ~~Schriftliche Weisungen des Auftragnehmers an den Unterauftragnehmer nach § 11 Abs. 2 BDSG (z.B. durch Vertrag der Datenverarbeitung im Auftrag)~~ |
| ☐ | ~~Vertragsstrafen bei Verstößen mit dem Auftragnehmer vereinbart~~ | ☐ | ~~Vertragsstrafen bei Verstößen mit dem Unterauftragnehmer vereinbart~~ |
| ☐ | Wirksame Kontrollrechte des Auftraggebers gegenüber dem Auftragnehmer vereinbart | ☐ | ~~Wirksame Kontrollrechte des Auftragnehmers gegenüber dem Unterauftragnehmer vereinbart~~ |
| ☐ | Sicherstellung der Vernichtung von Daten durch Auftraggeber und Auftragnehmer nach Beendigung des Auftrags | ☐ | Sicherstellung der Vernichtung von Daten durch Auftragnehmer und Unterauftragnehmer nach Beendigung des Auftrags gemäß schriftlicher Weisung des Auftraggebers |
| ☒ | Vertrag zwischen Auftraggeber und Auftragnehmer zum Einsatz von Unterauftragnehmern beim Auftragnehmer |
| ☒ | sonstiges: Weitere Maßnahmen zur Auftragskontrolle siehe Eingabekontrolle. Soweit zwischen Auftraggeber und Auftragnehmer vertraglich nicht anders vereinbart, bedarf der Einsatz von Unterauftragnehmern zur Ausführung der vom Auftraggeber an den Auftragnehmer übergebenen Arbeiten, der schriftlichen Zustimmung des Auftraggebers. Es wird auf den diesem Vertrag zugrundeliegenden Dienstleistungsvertrag zwischen Auftraggeber und Auftragnehmer verwiesen. |

1. **Verfügbarkeit**

Maßnahmen, die gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Siehe 1) a) – c) und 2) b) – c).

1. **Authentizität**

Maßnahmen, die gewährleisten, dass personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können.

* 1. **Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System | ☒ | Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |
| ☒ | Festlegung von Datenbankrechten | ☐ | ~~Versehen der Datensätze mit Zweckattributen/Datenfeldern~~\* |
| ☒ | Logische Mandantentrennung (software-seitig) | ☒ | Trennung von Produktiv- und Testsystem |
| ☒ | sonstiges: siehe 2) a) Eingabekontrolle. Die Trennungskontrolle obliegt der Maßgabe des Auftraggebers. Wurde mit dem Auftraggeber nicht anderes vereinbart, erfolgt die Datenverarbeitung logisch und physikalisch getrennt.  |

1. **Revisionsfähigkeit**

Maßnahmen, die gewährleisten, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Siehe 2) a) – c) und 4) a).

1. **Transparenz**

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können.