isdacom GmbH

Audit-Checkliste:

„Technische und organisatorische Maßnahmen (TOMs)“ nach Art. 32 DSGVO

zwecks

Überprüfung Auftragsverarbeiter: _____

_____

_____

Durch: _____

_____

_____

_____
Datum

Folgende technische und organisatorische Maßnahmen wurden vom Auftragsverarbeiter getroffen und vom Auftraggeber anhand dieser Checkliste überprüft (zutreffendes bitte ankreuzen):

Vertraulichkeit

(Artikel 32 Abs. 1 lit. b DSGVO)
„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; […]“

Checkliste Zutrittskontrolle

(es sind Maßnahmen zu treffen die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren)

Technische und organisatorische Maßnahmen:

☐ Alarmanlage für ☐ Gelände ☐ Gebäude für ☐ während ☐ nach der Arbeitszeit
☐ Wachdienst für ☐ Gelände ☐ Gebäude für ☐ während ☐ nach der Arbeitszeit
☐ Videoüberwachung für ☐ Gelände ☐ Gebäude für ☐ während ☐ nach der Arbeitszeit
↳ ☐ Monitoring ☐ Speicherung der Videoaufzeichnung
☐ Manuelles Schließsystem ☐ Automatisches Schließsystem ☐ Biometrisches Schließsystem
↳ ☐ Schlüssel nicht duplizierbar ☐ Sperre Codekarten möglich
☐ Zutrittskontrolle mittels Pförtner / Empfang
☐ Besucher werden protokolliert ☐ und erhalten einen Besucherausweis
☐ Schlüsselbuch für Schlüssel ☐ Ausgabebuch für Chipkarten ☐ Ausgabebuch für Transponder
↳ ☐ Überzählige Schlüssel, Chipkarten, Transponder werden sicher (z.B. in Schlüsselkästen) aufbewahrt

Paraphe/n: _____

☐ Server / Firewalls ☐ befinden sich in einem abgeschlossenen Raum ☐ sind ausgelagert
☐ Server / Firewalls sind gegen Zutritt Unbefugter geschützt

☐ sonstiges: _____

☐ sonstiges: _____

Checkliste Zugangskontrolle

(es sind Maßnahmen zu treffen die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können)

Technische und organisatorische Maßnahmen:

☐ Server sind gegen unbefugten Zugang geschützt
- ☐ Bootschutz ☐ Schnittstellenabsicherung ☐ Keine Laufwerke (CD, DVD, USB) vorhanden
- ☐ Firewall(s) ☐ Anti-Viren-Software ☐ VPN-Technologie

☐ Endgeräte sind gegen unbefugten Zugang geschützt
- ☐ Bootschutz ☐ Schnittstellenabsicherung ☐ Keine Laufwerke (CD, DVD, USB) vorhanden
- ☐ Firewall(s) ☐ Anti-Viren-Software ☐ VPN-Technologie
- ☐ zentralisierte Mobilgeräteverwaltung mittels Software

☐ Per Richtlinie ist verboten, auf Endgeräte / Server eigene bzw. ungeprüfte Dateien aufzuspielen
- ☐ Laptops eingeschlossen oder mit Kensington-Schloss gesichert ☐ PC-Gehäuse verschlossen
- ☐ Nutzung und Aufbewahrung mobiler Endgeräte durch Richtlinie geregelt

☐ Zugangskontrolle mittels Berechtigungen
- ☐ Benutzer + Passwort ☐ Benutzer + Hardware-Authentifikation ☐ Benutzer + Biometrie

☐ Zugangsberechtigungen werden individuell nach Erfordernis eingerichtet
☐ Endgeräte werden mittels Softwareverriegelung (Bildschirmschoner) geschützt
- Softwareverriegelung wird mittels ☐ Passwort ☐ Biometrie ☐ sonstiges _____ aufgehoben

☐ Softwareverriegelung schaltet sich nach _____ Minuten automatisch ein
☐ Passwortregelungen für sichere Passwörter werden maschinell erzwungen
☐ Eine Passwortrichtlinie gibt Auskunft über sichere Passwortmerkmale
☐ Datenträger ☐ mobile Datenträger ☐ Smartphones sind verschlüsselt

☐ sonstiges: _____

☐ sonstiges: _____

Checkliste Zugriffskontrolle

(es sind Maßnahmen zu treffen die geeignet sind, zu 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)

Technische und organisatorische Maßnahmen:

☐ Daten sind gegen (zufälligen) unbefugten Einblick geschützt
- ☐ automatische Softwareverriegelung (vgl. Zugangskontrolle) ☐ manuelle Softwareverriegelung

☐ Daten sind gegen (zufälligen) unbefugten Einblick geschützt
- ☐ Clean Desk ☐ Blickdichte / geschlossene Bürotüren ☐ Jalousien

☐ Jeder Benutzer greift nur auf diejenigen Dienste zu, die er zur Erfüllung seiner Aufgaben benötigt
- ☐ technisches Berechtigungskonzept ☐ Systemseitige Sanktionen bei Missbrauchsversuch: _____

☐ Jeder Benutzer greift nur auf diejenigen Dienste zu, die er zur Erfüllung seiner Aufgaben benötigt
- ☐ Berechtigungsvergabe nach 4-Augen-Prinzip ☐ Standardisierte Rechtevergabe (nicht auf Zuruf)

☐ Es existieren Zusatzpasswörter für besonders wichtige Funktionen (Administration)
- ☐ Standardpasswörter wurden geändert ☐ Verschlüsselte Übertragung der Passwörter im Netzwerk

☐ Es existieren Zusatzpasswörter für besonders wichtige Funktionen (Administration)
- ☐ Die sichere Aufbewahrung der Passwörter ist schriftlich geregelt

Paraphe/n: _____

- ☐ Anzahl der Administratoren ist auf ein Mindestmaß begrenzt
- ☐ Es existiert eine Richtlinie für den Umgang mit mobilen Endgeräten (Laptops, Smartphones, USB-Sticks)
  - ☐ Endgeräte sind verschlüsselt
- ☐ Es existiert eine Richtlinie für den Umgang mit mobilen Endgeräten (Laptops, Smartphones, USB-Sticks)
  - ☐ Ausgabe und Rücknahme werden dokumentiert ☐ Endgeräte werden verschlossen aufbewahrt
- ☐ Es ist sichergestellt, dass Löschfristen eingehalten werden
  - ☐ Erinnerungsmanagement in der EDV
  - ☐ Datenlöschungen werden protokolliert
- ☐ Es ist sichergestellt, dass Löschfristen eingehalten werden
  - ☐ Löschfristen sind in der internen Verarbeitungsübersicht aufgeführt
  - ☐ Es wird ein Protokollbuch über die Löschungen geführt
  - ☐ Datenlöschung erfolgt durch externes Unternehmen ➲ ☐ Übergabe wird protokolliert
    - ☐ Es wurde eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO abgeschlossen
- ☐ Datenträger werden vor Wiederverwendung bereinigt, evtl. Restdaten datenschutzkonform gelöscht
- ☐ Datenträger nicht wiederverwendet, sondern datenschutzkonform physisch zerstört
  - ☐ Datenträgervernichtung erfolgt durch externes Unternehmen ➲ ☐ Übergabe wird protokolliert
    - ☐ Es wurde eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO abgeschlossen

☐ sonstiges: _____

☐ sonstiges: _____

Checkliste Trennungsgebot

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)

Technische und organisatorische Maßnahmen:

- ☐ Daten verschiedener Kunden/Mandanten werden getrennt voneinander gespeichert
  - ☐ Logische Trennung (Separierung auf Verzeichnisebene)
  - ☐ Physische Trennung (Separierung auf verschiedenen Speichermedien wie HDDs oder CDs)
- ☐ Daten verschiedener Kunden/Mandanten werden getrennt voneinander abgelegt.
  - ☐ Logische Trennung (Separierung in einem Aktenordner mittels Trennlaschen)
  - ☐ Physische Trennung (Separierung auf verschiedene Aktenordner)
- ☐ Bei pseudonymisierten Daten wird der Schlüssel stets in einem getrennten System aufbewahrt
- ☐ Backups werden nach Kunden/Mandanten getrennt durchgeführt um Löschfristen entsprechen zu können
- ☐ Das Archiv ist nach Kunden/Mandanten getrennt um Löschfristen entsprechen zu können
- ☐ Das Testsystem ist strikt vom Echtsystem getrennt, so dass eine Datendurchmischung nicht möglich ist
- ☐ Es existiert eine Dokumentation für die Datenerhebung und Datenverarbeitung
- ☐ Es existiert eine Dokumentation der Archivierung und Recherche
- ☐ Es existiert eine Dokumentation der Datenbankrechte

☐ sonstiges: _____

☐ sonstiges: _____

Paraphe/n: _____

isdacom GmbH

Integrität

(Artikel 32 Abs. 1 lit. b DSGVO)

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; […]“

Checkliste Weitergabekontrolle

(es sind Maßnahmen zu treffen die geeignet sind, zu 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)

Technische und organisatorische Maßnahmen:

- ☐ Datenaustausch ☐ Datenträgertransporte finden statt
  - ☐ Datenträger sind beim Datenträgeraustausch stets verschlüsselt
  - ☐ Emails sind verschlüsselt ☐ Dateianhänge sind verschlüsselt
  - ☐ Daten werden nach Möglichkeit ☐ pseudonymisiert ☐ anonymisiert
- ☐ Datenaustausch ☐ Datenträgertransporte finden statt
  - ☐ Datenträgertransporte werden dokumentiert ☐ Datenträgerübergabe erfolgt stets gegen Quittung
  - ☐ Es werden sichere Transportbehälter/ -verpackungen genutzt
  - ☐ Pseudonyme sind durch geeignete Maßnahmen gegen Aufdeckung so gut wie möglich geschützt
- ☐ Es werden öffentliche Netzwerke genutzt (zum Beispiel WLAN-Hotspots)
  - ☐ Mobile Endgeräte werden auf „öffentliches Netzwerk“ umgestellt
  - ☐ Mobile Endgeräte verbinden sich zunächst via VPN und stellen erst dann die Internetverbindung her
- ☐ Es werden öffentliche Netzwerke genutzt (zum Beispiel WLAN-Hotspots)
  - ☐ Eine Richtlinie regelt den Umgang mit öffentlichen Netzwerken
- ☐ Fernwartungen werden durchgeführt und ein Zugriff auf personenbezogene Daten ist nicht ausgeschlossen
  - ☐ Es erfolgt ein ☐ Monitoring eine ☐ Protokollierung der Fernwartungsaktivitäten
    - ☐ Es wurde eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO abgeschlossen
- ☐ Fernwartungen werden durchgeführt und ein Zugriff auf personenbezogene Daten ist nicht ausgeschlossen
  - ☐ Das Benutzerpasswort wird nach jeder Fernwartung geändert

☐ sonstiges: _____

☐ sonstiges: _____

Checkliste Eingabekontrolle

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

Technische und organisatorische Maßnahmen:

- ☐ Die ☐ Eingabe ☐ Änderung ☐ Löschung von personenbezogenen Daten wird protokolliert
  - ☐ Die Protokolle werden ☐ verschlüsselt ☐ in einer sicheren Serverumgebung aufbewahrt
  - ☐ Sämtliche Aktivitäten der Netzverwaltung werden protokolliert
- ☐ Die ☐ Eingabe ☐ Änderung ☐ Löschung von personenbezogenen Daten wird protokolliert
  - ☐ Anweisung regelt über das übliche Maß hinausgehende Auswertungen nach Sicherheitsverstößen
  - ☐ Die Protokolle werden sicher verschlossen aufbewahrt
  - ☐ Für die Protokolle ist eine Löschfrist definiert
- ☐ Für die ☐ Eingabe ☐ Änderung ☐ Löschung von personenbezogenen Daten existieren Anweisungen
- ☐ Die elektronische Signatur zur Gewährleistung der Authentizität wird genutzt
- ☐ sonstiges: _____

☐ sonstiges: _____

Paraphe/n: _____

isdacom GmbH

Verfügbarkeit und Belastbarkeit

(Artikel 32 Abs. 1 lit. b DSGVO)
„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; […]“
(Artikel 32 Abs. 1 lit. d DSGVO)
„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; […]“

Checkliste Verfügbarkeitskontrolle

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind)

Technische und organisatorische Maßnahmen:

- ☐ Bei Störfällen ist eine automatische Alarmierung gewährleistet
- ☐ Bei Störfällen werden die getroffenen (Gegen)Maßnahmen revisionssicher dokumentiert
- ☐ Es ist bekannt, wie lange im Notfall auf das Netzwerk verzichtet werden kann
  - ☐ Ein Notbetrieb kann innerhalb eines vertretbaren Zeitraums initiiert werden
  - ☐ Notbetrieb erfolgt mittels Austauschkomponenten
  - ☐ Notbetrieb erfolgt mittels Ausweichrechenzentrum
- ☐ Für den Fall eines Netzwerkausfalls gibt es eine detaillierte Beschreibung der Wiederanlaufmaßnahmen
- ☐ Es existiert (jeweils) ein aktuelles Notfallkonzept für folgende Bereiche:
  - ☐ _____
- ☐ Es existiert ein Konzept für die Datensicherungen und Datenwiederherstellungen
  - ☐ Die Datenwiederherstellung wird regelmäßig (mindestens halbjährlich) getestet
- ☐ Datensicherungen werden ausgelagert und befinden sich mindestens in einer anderen Brandschutzzone
- ☐ Eine Unterbrechungsfreie Stromversorgung (USV) schützt ☐ den Server ☐ die Arbeits-PCs
- ☐ Es befinden sich Feuer- und Rauchermelder ☐ im Serverraum ☐ in den PC-Arbeitsräumen
- ☐ Es befinden sich Feuerlöscher ☐ im Serverraum ☐ in den PC-Arbeitsräumen
- ☐ Eine Klimaanlage kühlt ☐ den Serverraum ☐ die PC-Arbeitsräume
- ☐ Es befinden sich Wasserschutzeinrichtungen ☐ im Serverraum ☐ in den PC-Arbeitsräumen
- ☐ Der Serverraum ist gegen unberechtigten Zugang geschützt ☐ und mit einer Alarmanlage verbunden
- ☐ Eine Richtlinie verbietet das Essen und Trinken ☐ im Serverraum ☐ an den PC-Arbeitsplätzen
- ☐ Es existiert ein Katastrophenarchiv, welches sich in einer anderen Brandschutzzone befindet
- ☐ Es existiert eine Dokumentation wie im Streikfall der Geschäftsbetrieb aufrechterhalten werden kann

☐ sonstiges: _____

☐ sonstiges: _____

Paraphe/n: _____

isdacom GmbH

Überprüfung, Bewertung und Evaluierung

(Artikel 32 Abs. 1 lit. d DSGVO)

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung; […]“

Checkliste Auftragskontrolle

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)

Technische und organisatorische Maßnahmen:

- ☐ Es gibt eine Übersicht, in der alle Datenverarbeitungen im Auftrag aufgeführt werden:
  - ☐ Für Datenverarbeitungen im Auftrag als Auftragnehmer
  - ☐ Für Datenverarbeitungen im Auftrag als Auftraggeber
- ☐ Die Vereinbarungen zur Datenverarbeitung im Auftrag sind stets schriftlich fixiert
- ☐ Es werden ☐ in der Regel ☐ keine Vertragsstrafen in der Vereinbarung aufgenommen
- ☐ Der AN wird sorgfältig durch _____ ausgewählt[1]
- ☐ Der AN wird vor Beginn der Tätigkeit und dann laufend überprüft
  - ☐ Die Prüfungen werden durch _____ durchgeführt[2]
  - ☐ Die Prüfungen werden in der Regel mittels _____ durchgeführt[3]
  - ☐ Die Prüfungen werden dokumentiert
- ☐ Der AN hat bestätigt, dass seine Mitarbeiter auf Vertraulichkeit verpflichtet worden sind
- ☐ Die TOMs des AN sind Bestandteil der Datenverarbeitung im Auftrag und liegen schriftlich vor
  - ☐ Zusätzlich liegt ein Datenschutz- und Datensicherheitskonzept vor
  - ☐ Zusätzlich liegt _____ vor[4]
- ☐ Die Einschaltung von Unterauftragnehmern ist klar geregelt
- ☐ Die Kompetenzen zwischen AG und AN sind klar und deutlich abgegrenzt
  - ☐ Die Weisungsbefugnis des AG ist stets Bestandteil der Vereinbarung mit dem AN
- ☐ Es wurden wirksame Kontrollrechte vereinbart
- ☐ Es ist sichergestellt, dass die personenbezogenen Daten nach Beendigung des Auftrags vernichtet werden
  - ☐ Durch den AN
  - ☐ Durch den AG nach Rückgabe durch den AN
- ☐ Die übrigen Forderungen aus dem Forderungskatalog (Art. 28 DSGVO) sind schriftlich fixiert

☐ sonstiges: _____

☐ sonstiges: _____

Mitwirkende Personen Auftraggeber:	Mitwirkende Personen Auftragnehmer:
_____	_____
_____	_____
_____	_____

Paraphe/n: _____

isdacom GmbH

↳ Die Auditierung fand als ☐ Vorortprüfung ☐ als Übersendung und Prüfung dieser Checkliste statt.

_____, _____ _____, _____
Ort Datum Ort Datum

_____ _____
(_____) (_____)

Erläuterungen:

Wenn von „Dokumentation“ die Rede ist, so ist immer eine schriftliche Arbeitsanweisung oder schriftliche Richtlinie gemeint

[1] Auswahl erfolgt beispielsweise durch Geschäftsführung oder Fachabteilung
[2] Prüfung wird beispielsweise vom Datenschutzbeauftragten und dem Leiter der Fachabteilung durchgeführt
[3] Prüfung erfolgt beispielsweise mittels Vor-Ort-Termin oder per Übersendung dieser Auditliste
[4] Weitere relevante Dokumente könnten beispielsweise ein IT-Sicherheitskonzept oder Datenschutzrichtlinien sein

Diese Audit-Checkliste fragt wesentliche Punkte ab, die zur Beurteilung der Datensicherheit das Mindestmaß darstellen und um somit einschätzen zu können, ob ein Auftragsverarbeiter die ihm übertragenen Aufgaben (nach Art. 32 DSGVO) datenschutzkonform erledigen kann. Sie ist bewusst nicht unternehmensbezogen, so dass sie branchenübergreifend für Kurz-Audits zum Einsatz kommen und beliebig angepasst und erweitert werden kann. Diese Audit-Checkliste stellt lediglich einen kleinen Auszug (kleiner 10%) der von uns genutzten Unterlagen dar. Sofern eine vollständige Aufnahme der technischen und organisatorischen Maßnahmen bei Ihrem Kunden oder Ihrem Unternehmen angezeigt oder erforderlich ist, kontaktieren Sie uns einfach, wir unterbreiten Ihnen gerne ein individuelles Angebot.

Mit freundlichen Grüßen

isdacom GmbH

Paraphe/n: _____