Arbeitsblatt: Technische und organisatorische Maßnahmen i. S. d. Art. 32 DSGVO (unter auslegender Betrachtung § 64 DSAnpUG- EU/ BDSG n. F.)

der

_____

_____ am Standort: _____

_____

Bearbeitungshinweise:
Bitte füllen Sie dieses Arbeitsblatt gesondert für jeden Standort Ihres Unternehmens aus und kreuzen Sie die zutreffenden technischen und organisatorischen Maßnahmen wahrheitsgemäß an. Bitte notieren Sie ergänzende oder beschreibende Bemerkungen in den Freizeilen oder geplante Einführungen unter Punkt 15. Bitte senden Sie dieses Arbeitsblatt ausgefüllt an die datarea GmbH zurück, vielen Dank.

Zu den elementaren Gewährleistungszielen der IT-Sicherheit zählen die Verfügbarkeit, Integrität und Vertraulichkeit. Daneben wurden im Rahmen der Reform durch die Europäische Datenschutz-Grundverordnung weitere Gewährleistungsziele mit Datenschutzbezug, wie die Nichtverkettbarkeit, Transparenz und Intervenierbarkeit sowie die Datenminimierung, entwickelt.

Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

- ☐ Manuelles Schließsystem
- ☐ Schließsystem mit Codesperre
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Systemauthentifikation mit Benutzername/Passwort
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher/Besucherbuch
- ☐ sorgfältige Auswahl von Sicherheitspersonal
- ☐ Einsatz von Anti-Viren-Software
- ☐ Einsatz einer Hardware-Firewall
- ☐ besondere Verschlussmaßnahmen Server
- ☐ besondere Verschlussmaßnahmen bei sensiblen personenbezogenen Daten z. B. Personal
- ☐ Sicherheitsschlösser
- ☐ Zugangssperre mit biometrischen Verfahren
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Einsatz von Virtual Private Network-Technologie (VPN)
- ☐ Personenkontrolle beim Pförtner/Empfang
- ☐ sorgfältige Auswahl von Servicepersonal (z.B. Reinigung)
- ☐ Tragepflicht von Mitarbeiter-/Gästeausweisen
- ☐ Einsatz einer Software-Firewall
- ☐ Verpflichtung eigener Mitarbeiter auf das Datengeheimnis
- ☐ besondere Verschlussmaßnahmen Archiv
- ☐ Alarmanlage

☐ Videoüberwachung ☐ Türspion oder Gegensprechanlage

Ergänzung/Besonderheit:_____

_____

_____

_____

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

☐ Verschlüsselung von mobilen Datenträgern (z.B. USB-Stick, Smartphone, Tablett, Externe Festplatte, Laptop)

☐ restriktiver Einsatz von mobilen Datenträgern

☐ Einsatz von zentraler Smartphone-Administrations-Software (z .B. zum externen Löschen von Daten)

☐ Schreib-/Leseschutz

Ergänzung/Besonderheit:_____

_____

_____

_____

3. *Speicherkontrolle*

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

☐ Erstellung eines Berechtigungskonzepts

☐ routinemäßige Löschung von nicht mehr benötigten Daten

☐ Richtlinien für die Dateiorganisation

☐ revisionssichere E-Mail-Archivierung

☐ Protokollierung der Dateibenutzung

☐ Kontrolle von Hilfsprogrammen, die geeignet sind Sicherungsmaßnahmen zu umgehen

☐ Verhinderung des Fotografierens einer Bildschirmanzeige

☐ Achtung auf datenschutzfreundliche Voreinstellungen in Systemen und Programmen

Ergänzung/Besonderheit:_____

_____

_____

_____

4. *Benutzerkontrolle*

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

☐ Erstellung von Benutzerprofilen

☐ Erstellung eines Berechtigungskonzepts

☐ differenzierte Zugriffsregelung (need to know-Prinzip)

☐ Netzwerkzugangskontrolle Netzwerk Network Access Control (NAC)

☐ Einsatz von Checklisten zur Ausgestaltung von Rollen und Berechtigungen von Mitarbeitern

Ergänzung/Besonderheit:_____

_____

_____

_____

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- ☐ Verwaltung der Rechte durch Systemadministrator
- ☐ nur die notwendige Anzahl an Administratoren einsetzen
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ ordnungsgemäße Vernichtung von Datenträgern
- ☐ sichere Aufbewahrung von Datenträgern
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Protokollierung der Vernichtung
- ☐ Einsatz von Aktenvernichtern
- ☐ Einsatz von Dienstleistern zur Entsorgung (nach Möglichkeit mit Zertifikat)
- ☐ Sperrung von externen Schnittstellen (USB etc.)
- ☐ verschließbare Aktenschränke
- ☐ Festlegung von Aufbewahrungsfristen für gespeicherte Daten
- ☐ differenzierte Archivbestände

Ergänzung/Besonderheit:_____

_____

_____

_____

6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- ☐ Einrichtung von Standleitungen bzw. VPN-Tunneln
- ☐ Weitergabe von Daten in pseudonymisierter Form (Identifikationsmerkmal wird durch ein Pseudonym, z. B. Buchstaben- oder Zahlenkombination, ersetzt – Wiederherstellbarkeit möglich)
- ☐ Erstellung einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Weitergabe von Daten in anonymisierter Form (keine Personenbezug mehr herstellbar)
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

Ergänzung/Besonderheit:_____

_____

_____

_____

7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten (Logfile)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☐ Einsatz einer E-Mail-Signatur zur Identifikation des Signaturersteller

Ergänzung/Besonderheit:_____

_____

_____

_____

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird.

- ☐ sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ sichere Transportbehälter/-verpackungen
- ☐ Festlegung von Transportpersonal und -wegen
- ☐ Anforderungen von Quittungen
- ☐ Gehäuseverriegelungen
- ☐ Schloss für mobile Datenträger als Diebstahlschutz
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ E-Mail-Verschlüsselung
- ☐ Versand von E-Mail-Anhängen passwortgeschützt oder via verschlüsseltem Archiv
- ☐ sicheres Internetprotokoll - Hypertext Transfer Protocol Secure (https)

Ergänzung/Besonderheit:_____

_____

_____

_____

9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- ☐ Testung der Datenwiederherstellbarkeit
- ☐ Erstellung eines Backup- & Recoverykonzepts
- ☐ Unterstützung der Datenportablität (strukturiertes/gängiges/maschinenlesbares/interoperables Format)
- ☐ Protokollierung und Auswertung von Störungsvorfällen

☐ Einsatz von Raid-Controllern (Redundant Array of Independent Disks)

☐ Einsatz von zentralem Netzwerk

☐ Einsatz von Cloud-Lösungen

Ergänzung/Besonderheit:_____

_____

_____

_____

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

☐ Anzeige von Fehler- und Störmeldungen in den IT-Systemen

☐ IT-Managementsystem zur Überwachung der IT-Asset-Lebenszyklen

☐ externe/interne technische Sicherheitsanalysen (T-Systeme, Infrastruktur oder Anwendungen)

☐ Penetrationstests (vertiefte Feststellung von Angriffen in die Infrastruktur)

☐ Einsatz von Intrusion-Detection-Systemen (Angriffserkennung)

☐ Auswertung von Aufzeichnungen und Protokolle der Detektionsmaßnahmen

☐ Test- und Freigabeverfahren z. B. bei Einführung neuer Soft- oder Hardware

☐ Sensibilisierungen der Mitarbeiter zum Datenschutz und/oder -sicherheit

Ergänzung/Besonderheit:_____

_____

_____

_____

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

☐ Erstellung eines Sicherheitskonzepts

☐ Managementsystem für Informationssicherheit (ISMS) gemäß DIN ISO/IEC 27001

☐ Einsatz eines Sicherheitsbeauftragten

☐ Aufgezeichnete und begründete Sicherheitsstrategie der Leitungsebene

Ergänzung/Besonderheit:_____

_____

_____

_____

12. Auftragskontrolle

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

- ☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- ☐ vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☐ schriftliche Datenschutzweisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag)
- ☐ Überprüfung der Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ☐ Überprüfung Bestellung eines Datenschutzbeauftragten beim Auftragnehmer
- ☐ Sicherstellung der Rückgabe/Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- ☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- ☐ Vertragsstrafen bei Verstößen
- ☐ Einsatz von Pflichtenheften

Ergänzung/Besonderheit:_____

_____

_____

_____

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- ☐ Sicherstellung unterbrechungsfreier Stromversorgung
- ☐ Serverräumen mit Klimaanlage/Abluftanlage
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Aufbewahrung von Datensicherung an einem sicheren, externen Ort
- ☐ keine umliegenden Wasserleitungen um Serverräume
- ☐ Erstellung eines Notfallplans/Notfallhandbuch
- ☐ Serverräume oberhalb der Wassergrenze im Falle eines Hochwassers

Ergänzung/Besonderheit:_____

_____

_____

_____

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ logische Mandantentrennung (softwareseitig)

☐ Erstellung eines Berechtigungskonzepts

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☐ versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☐ Festlegung von Datenbankrechten

☐ Trennung von Produktiv- und Testsystem

Ergänzung/Besonderheit:_____

_____

_____

_____

15. Sonstiges/geplante Maßnahmen

_____

_____

_____

_____

_____

_____

_____

_____

_____
Verantwortlicher für die Erstellung in Druckbuchstaben

_____, den _____

_____
Unterschrift Verantwortlicher für die Erstellung