Maßnahmen des Auftragnehmers gemäß Art. 32 DSGVO (Sicherheit der Verarbeitung)

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

Technisch
O Alarmanlage
O Absicherung von Gebäudeschächten
O Automatisches Zugangskontrollsystem
O Chipkarten-/Transponder-Schließsystem
O Schließsystem mit Codesperre
O Manuelles Schließsystem
O Biometrische Zugangssperren
O Videoüberwachung der Zugänge
O Lichtschranken / Bewegungsmelder
O Sicherheitsschlösser
O Türen mit Knauf Außenseite
O Klingelanlage mit Kamera
Sonstige:

Organisatorisch
O Schlüsselregelung (Schlüsselausgabe etc.)
O Personenkontrolle beim Pförtner / Empfang
O Protokollierung der Besucher
O Sorgfältige Auswahl von Reinigungspersonal
O Sorgfältige Auswahl von Wachpersonal
O Tragepflicht von Berechtigungsausweisen
O Besucher in Begleitung durch Mitarbeiter

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

Technisch
O Zuordnung von Benutzerrechten
O Erstellen von Benutzerprofilen
O Passwortvergabe
O Authentifikation mit biometrischen Verfahren
O Authentifikation mit Benutzername / Passwort
O Zuordnung von Benutzerprofilen zu IT-Systemen
O Gehäuseverriegelungen

O Einsatz von VPN-Technologie
O Sperren von externen Schnittstellen (USB etc.)
O Sicherheitsschlösser
O Antivirensoftware Server
O Antivirensoftware Client
O Antivirensoftware mobile Geräte
O Verschlüsselung von Datenträgern in Laptops / Notebooks
O Einsatz einer Hardware-Firewall
O Einsatz einer Software-Firewall
O Verschlüsselung von mobilen Datenträgern
O Verschlüsselung von Smartphone-Inhalten

organisatorisch
O Verwalten von Benutzerberechtigungen
O Erstellen von Benutzerprofilen
O Zentrale Passwortvergabe
O Richtlinie „Sicheres Passwort“
O Richtlinie „Löschen / Vernichten“
O Richtlinie „Clean desk“
O Allg. Richtlinie Datenschutz und / oder Sicherheit
O Mobile Device Policy
O Anleitung „Manuelle Desktopsperre“

O Gehäuseverriegelung
O BIOS Schutz (separates Passwort)
O Automatische Desktopsperre
O Einsatz von zentraler Smartphone-Administrations-Software
(z.B. zum externen Löschen von Daten)

Sonstige:

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.)

O Erstellen eines Berechtigungskonzepts
O Verwaltung der Rechte durch Systemadministrator
O Anzahl der Administratoren auf das "Notwendigste" reduziert
O Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
O Protokollierung von Zugriffen auf Anwendungen,
insbesondere bei der Eingabe, Änderung und Löschung von Daten
O Sichere Aufbewahrung von Datenträgern
O physische Löschung von Datenträgern vor Wiederverwendung
O ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
O Einsatz von Aktenvernichtern bzw. Dienstleistern
(nach Möglichkeit mit Datenschutz-Gütesiegel, mind. Stufe 3, cross cut)
O Protokollierung der Vernichtung
O Verschlüsselung von Datenträgern
O Datenschutztresor
O Verwaltung Benutzerrechte durch Administratoren

Sonstige:

Pseudonymisierung

O Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)
O Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

Sonstige:

Weitergabekontrolle
(Maßnahmen, die 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.)

O Einrichtungen von Standleitungen bzw. VPN-Tunneln
O Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
O E-Mail-Verschlüsselung
O Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
O Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
O Beim physischen Transport: sichere Transportbehälter/-verpackungen
O Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
O Nutzung von Signaturverfahren
O Bereitstellung über verschlüsselte Verbindungen wie sftp, https

Sonstige:

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

O Protokollierung der Eingabe, Änderung und Löschung von Daten
O Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
O Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
O Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
O Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
O Klare Zuständigkeiten für Löschungen

Sonstige:

Verfügbarkeit und Belastbarkeit
(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

O Unterbrechungsfreie Stromversorgung (USV)
O Klimaanlage in Serverräumen
O Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
O Schutzsteckdosenleisten in Serverräumen
O Feuer- und Rauchmeldeanlagen
O Feuerlöschgeräte in Serverräumen
O Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
O Erstellen eines Backup- & Recoverykonzepts
O Testen von Datenwiederherstellung
O Erstellen eines Notfallplans
O Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
O Serverräume nicht unter sanitären Anlagen

O Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)
O RAID System / Festplattenspiegelung
O Videoüberwachung Serverraum
O Getrennte Partitionen für Betriebssysteme und Daten

Sonstige:

Trennungsgebot
(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)

O physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
O Logische Mandantentrennung (softwareseitig)
O Erstellung eines Berechtigungskonzepts
O Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
O Versehen der Datensätze mit Zweckattributen/Datenfeldern
O Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und Aufbewahrung auf einem getrennten, abgesicherten IT-System
O Festlegung von Datenbankrechten
O Trennung von Produktiv- und Testsystem
O Datensätze sind mit Zweckattributen versehen

Sonstige:

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management
O Software-Lösungen für Datenschutz-Management im Einsatz
O Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)
O Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12
O Anderweitiges dokumentiertes Sicherheits-Konzept
O Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
O Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
O Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
O Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
O Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
O Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
O Verantwortlicher kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
O formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Sonstige:

Incident-Response-Management (Reaktion auf Sicherheitsverletzungen)

Technische Maßnahmen
O Einsatz von Firewall und regelmäßige Aktualisierung
O Einsatz von Spamfilter und regelmäßige Aktualisierung
O Einsatz von Virenscanner und regelmäßige Aktualisierung
O Intrusion Detection System (IDS)
O Intrusion Prevention System (IPS)

Organisatorische Maßnahmen
O Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
O Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
O Einbindung von **O** DSB und **O** ISB in Sicherheitsvorfälle und Datenpannen
O Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
O Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Sonstige:

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

O Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
O Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

Sonstige:

Auftragskontrolle (Outsourcing an Dritte)
(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)

O Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
O vorherige Prüfung der und Dokumentation der beim Auftragnehmer
O getroffenen Sicherheitsmaßnahmen schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DSGVO
O Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
O Auftragnehmer hat Datenschutzbeauftragten bestellt
O Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
O schriftliche Weisungen an den Auftragnehmer
O Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
O Regelung zum Einsatz weiterer Subunternehmer
O laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
O Vertragsstrafen bei Verstößen

Sonstige:

---

alternativ:

O Hiermit versichere/n ich/wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.

Kanzlei:
Burkhard Goßens Rechtsanwälte
Ahornallee 10 - 14050 Berlin

Tel.: +49 30 30 61 41 42
Fax: +49 30 30 61 41 43
https://gossens.de/

Alternativ (ganz kleine Variante/hier besteht in der Regel Ergänzungsbedarf):

O Automatische Updates im Betriebssystem aktivieren

O Automatische Updates des Browsers aktivieren

O Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte

O Standard-Gruppenverwaltung (z. B. in Windows)

O Aktueller Virenscanner/Sicherheitssoftware

O Papieraktenvernichtung mit Standard-Shredder

O Abrechnungs- und Recherche-PC trennen

O Zugriffs- und Berechtigungskonzept

O Ende-zu-Ende und Transportverschlüsselung bei elektronischer Übermittlung von Gesundheitsdaten an Kostenträger bzw. Prüfdienste

Kanzlei:
Burkhard Goßens Rechtsanwälte
Ahornallee 10 - 14050 Berlin

Tel.: +49 30 30 61 41 42
Fax: +49 30 30 61 41 43
https://gossens.de/