Anlage 2 - Technische und organisatorische Maßnahmen

Verantwortliche für die Datenverarbeitung sind gem. Art. 32 DSGVO verpflichtet, technische und organisatorische Maßnahmen zu treffen, durch die die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet wird. Maßnahmen müssen dabei so gewählt sein, dass durch sie in der Summe ein angemessenes Schutzniveau sichergestellt wird. Diese Übersicht erläutert vor diesem Hintergrund, welche konkreten Maßnahmen durch den Auftragnehmer im Hinblick auf die Verarbeitung personenbezogener Daten im konkreten Fall getroffen sind.

Weisungen zu technischen und organisatorischen Maßnahmen

1. Organisation der Informationssicherheit

Es sind Richtlinien, Prozesse und Verantwortlichkeiten festzulegen, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.

Maßnahmen:

☒ Informationssicherheitsrichtlinie.

☒ Anwenderrichtlinien für den Umgang mit Geräten und dem Verhalten bei der Nutzung von Informationstechnologie.

☒ Prozesse für die Verwaltung von Datenträgern und Entsorgung von Datenträgern.

☐ Festlegung der Rollen und Verantwortlichkeiten für Betrieb von Anwendungen und System, Datenschutz und Informationssicherheit.

☒ Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses.

☐ Regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

2. Privacy by Design

Privacy by Design beinhaltet den Gedanken, dass Systeme so konzipiert und konstruiert sein sollten, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein.

Maßnahmen:

☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

☐ Prozess zur Sicherstellung von Privacy by Design bei Einführung oder Änderung von Systemen und Anwendungen.

☒ Die Verarbeitungen und Systeme sind so konzipiert, dass Sie ein DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ermöglichen und sicherstellen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

3. Privacy by Default

Privacy by Default bezieht sich auf die datenschutzfreundlichen Voreinstellungen / Standardeinstellungen. Inwieweit wurden diese von Ihnen vorgenommen? Beispiel: Bei einem Besuch einer Webseite kann der Besucher erwarten, dass alle Programme zunächst deaktiviert sind, die personenbezogene Daten erheben.

Maßnahmen:

☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen.

☐ Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert.

☒ Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins).

Weisungen zu technischen und organisatorischen Maßnahmen

Weitere umgesetzte Maßnahmen / Erläuterungen:

4. Zugriffskontrolle und Zugangskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik. Bei Online-Zugriffen ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.). Der Auftragnehmer gewährleistet, dass die zur Benutzung von IT-Infrastruktur berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind, und dass personenbezogene Daten bei der Verarbeitung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Maßnahmen:

- ☒ Berechtigungskonzepte dokumentiert.
- ☒ Vermeidung von Gruppenusern.
- ☒ Zugriff auf Daten ist eingeschränkt und nur für Berechtigte möglich.
- ☒ Sperrung des Benutzerkontos bei Fehlversuchen / Inaktivität.
- ☒ Sperrung des Endgerätes bei Verlassen des Arbeitsplatzes oder Inaktivität.
- ☒ Anzahl der Administratoren auf das „Notwendigste" reduziert.
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- ☐ Umsetzen eines Prozesses zur Berechtigungsvergabe.
- ☒ Regelmäßige Überprüfung der Berechtigungen.
- ☒ Passwortrichtlinie, Implementierung komplexer Passwörter.
- ☐ Einsatz starker Authentifizierung mit mindestens 2 Faktoren aus Wissen, Besitz, Eigenschaften (Pin, Token, Smartcard, biometrische Verfahren).

Weitere umgesetzte Maßnahmen / Erläuterungen:

5. Kryptographie und / oder Pseudonymisierung

Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen.

Maßnahmen, die geeignet sind, eine Identifikation des Betroffenen zu erschweren.

Maßnahmen:

- ☐ Organisatorische Anweisung für die Verschlüsselung von Daten.
- ☐ Verschlüsselung von Datenträgern (z.B. mobile Festplatten, USB-Sticks etc.).
- ☐ Verschlüsselung von Endgeräten (PC, Laptop, Smartphones).
- ☒ Verschlüsselte Ablage von personenbezogenen Daten.
- ☐ Verschlüsselung von Datensicherungsmedien (z.B. Bänder, Festplatten etc.).
- ☒ Verschlüsselung von Zugängen zum Netzwerkzugängen und -verbindungen.
- ☒ Einsatz von Pseudonymen, Verfahren zur Pseudonymisierung von Daten.
- ☒ Einsatz Verfahren zur Anonymisierung von Daten.

Weitere umgesetzte Maßnahmen / Erläuterungen:

Weisungen zu technischen und organisatorischen Maßnahmen

6. Schutz von Gebäuden

Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung. Der Auftragnehmer trifft Maßnahmen, um zu verhindern, dass unbefugte Personen Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten mit denen personenbezogene Daten verarbeitet werden.

Maßnahmen:

- ☐ Zonenkonzept und Festlegung von Sicherheitsbereichen.
- ☐ Gebäudesicherung durch Zäune.
- ☐ Sicherheitsschlösser und Schlüsselverwaltung / Protokollierung der Schlüsselausgabe
- ☐ Einsatz von Schliess- und Zutrittssystemen (Chipkarten- / Transponder-Schließsystem, Codesicherung etc.).
- ☐ Alarmanlage.
- ☐ Videoüberwachung.
- ☐ Lichtschranken / Bewegungsmelder.
- ☐ Einsatz von Wachpersonal.
- ☐ Mitarbeiter- /Besucherausweise.
- ☒ Regelung für den Umgang mit Besuchern.
- ☒ Anmeldung für Besucher (Empfang).
- ☒ Kontrolle von Besuchern (Pförtner/Empfang).
- ☐ Protokollierung von Besuchern (Besucherbuch).

Weitere umgesetzte Maßnahmen / Erläuterungen:

Es werden keine Personenbezogenen Daten auf den Endgeräten gespeichert.

7. Schutz von Betriebsmitteln / Informationswerten

Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation.

Maßnahmen:

- ☒ Sichere Platzierung der Systeme, so dass Schutz vor Diebstahl gewährleistet ist.
- ☒ Schutz der Betriebsmittel vor Feuer, Wasser oder Überspannung.
- ☒ Ablage von Akten und Dokumente in verschlossenen Büros, Aktenschränken.
- ☐ Unterbringung der Server- und Netzkomponenten in gesicherten Räumen, Schränken etc.
- ☐ Regelmäßige Wartung der Betriebsmittel.
- ☒ Sichere Löschung, Vernichtung und Entsorgung von Betriebsmitteln.

Weitere umgesetzte Maßnahmen / Erläuterungen:

8. Betriebsverfahren und Zuständigkeiten

Sicherstellung des ordnungsgemäßen und sicheren Betriebes von Systemen sowie Verfahren zur Verarbeitung von Informationen.

Maßnahmen:

☐ Dokumentierte Sytemkonfigurationen und Betriebsverfahren, Betriebsführunghandbücher.

☒ Klare Zuordnung von Verantwortlichkeiten für die System- und Anwendungsbetreuung.

☒ Trennung der Verarbeitung von Daten der einzelnen Mandanten.

☒ Trennung von Entwicklungs-, Test- und Produktivsystemen.

☒ Überwachung des Systembetriebs und der Anlagen.

☒ Wartungsverträge mit geeigneter Reaktionszeit

☐ Einsatz von Systemen zur Verwaltung von Systemen und Geräten (Assetmanagement, Mobile Device Management, Softwareverwaltung und -verteilung).

Weitere umgesetzte Maßnahmen / Erläuterungen:

9. Datensicherungen

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

☒ Datensicherungskonzept mit regelmäßigen Backups.

☐ Auslagerung der Backup in andere Brandzonen.

☒ Auslagerung der Backups in andere Gebäude.

☒ Regelmäßige Tests der Datensicherung und Wiederherstellung von Daten, Anwendungen und Systemen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

10. Schutz vor Malware und Patchmanagement

Verhinderung einer Ausnutzung technischer Schwachstellen durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines Patchmanagements.

Maßnahmen:

☒ Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen.

☒ Einsatz von Anti-Malware-Software.

☒ Regelmäßige Einspielen von Sicherheitspatches und Updates.

Weitere umgesetzte Maßnahmen / Erläuterungen:

11. Protokollierung und Überwachung

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind. (Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.)

Maßnahmen:

- ☒ Protokollieurng von Aktivitäten der Systemadministratoren.
- ☒ Überwachung der Systemnutzung.
- ☐ Protokollierung von Zugängen.
- ☒ Protokollierung von Zugriffen.
- ☒ Auswertung von Log-Dateien.

Weitere umgesetzte Maßnahmen / Erläuterungen:

12. Netzwerksicherheitsmanagement

Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden.

Maßnahmen:

- ☐ Einsatz von Netzwerkmanagementsoftware.
- ☒ Einsatz von Firewallsystemen.
- ☐ Einsatz von Intrusion Detection / Intrusion Prevention Systemen.
- ☒ Benutzerauthentifizierung und Verschlüsselung von externen Zugriffen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

13. Informationsübertragung

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft sowie festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen sowie Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
(Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Maßnahmen:

- ☒ Regelungen für den Austausch sensibler Informationen und Beschränkung des zur Übermittlung befugten Personenkreises.
- ☒ Weitergabe von Daten an Dritte nur nach Prüfung der Rechtsgrundlage.
- ☒ Rechtmäßigkeit und schriftliche Festlegung der Weitergabe von Daten in Drittländer.
- ☒ Sichere Datenübertragung zwischen Client und Server.
- ☒ Angemessener Schutz von Emails, die sensible Informationen / Daten beeinhalten.
- ☒ Einsatz von verschlüsselten externen Zugriffen.
- ☒ Sicherer Transport und Versand von Datenträgern, Daten und Dokumenten.

Weitere umgesetzte Maßnahmen / Erläuterungen:

14. Netztrennung

Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.

Maßnahmen:

☒ Logische Mandantentrennnung.

☐ Datentrennung durch Segmentierung von Netzwerken unterschiedlicher Mandanten.

☒ Trennung der Netze bei Remote Zugriffen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

15. Anschaffung, Entwicklung und Instandhaltung von Systemen

Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist.

Maßnahmen:

☒ Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme.

☐ Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen.

☒ Leitlinien zur sicheren Systementwicklung.

☐ Überwachung von ausgelagerten Systementwicklungstätigkeiten.

☒ Schutz von Testdaten.

Weitere umgesetzte Maßnahmen / Erläuterungen:

16. Lieferantenbeziehungen

Maßnahmen betreffend die Informationssicherheit zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf die Werte des Unternehmens, sollten mit Sublieferanten / Subunternehmern vereinbart und dokumentiert werden.

Maßnahmen:

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).

☒ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. DSGVO der Auftragnehmer hat Datenschutzbeauftragten bestellt.

☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart.

☐ Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen.

☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.

☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

☐ Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.

☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

Weitere umgesetzte Maßnahmen / Erläuterungen:

17. Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall etc.) zu implementieren.

Maßnahmen:

☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

☒ Sofortige Information des Auftraggebers bei Datenschutzvorfällen.

☐ Einbindung des Datenschutz- und Informationssicherheitsbeauftragten bei Datenschutzvorfällen.

☐ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

18. Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements

Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen, wie Krisen- oder Schadensfälle. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Maßnahmen:

☒ Einsatz redundanter Systeme.

☒ Einsatz redundanter Systeme an räumlich getrennten Standorten (z.B. Notfall-Rechenzentrum).

☐ Dokumentierte Notfallpläne.

☐ Regelmäßige Tests bzgl. der Wirksamkeit der Notfallmaßnahmen.

☒ Frühzeitige Information des Auftraggebers bei Notfällen.

Weitere umgesetzte Maßnahmen / Erläuterungen:

19. Einhaltung gesetzlicher und vertraglicher Anforderungen

Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen.

Maßnahmen:

☒ Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit.

☒ Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende.

☐ Einrichtung eines Lizenzmanagements.

☒ Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten und Dienstleistern.

Weitere umgesetzte Maßnahmen / Erläuterungen:

20. Datenschutzanforderungen und Datenschutzmanagement

Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollte entsprechend den Anforderungen der einschlägigen gesetzlichen Regelungen, anderen Vorschriften sowie Vertragsbestimmungen sichergestellt werden.

Maßnahmen:

- ☐ Bestellung eines Datenschutzbeauftragten.
- ☒ Verzeichnis der Verarbeitungstätigkeiten.
- ☒ Datenschutzfolgeabschätzung für Verfahren, die sensible Informationen / Daten verarbeiten.
- ☐ Durchführung von Datenschutzschulungen.
- ☐ Aufbau eines Datenschutz-Managementsystems.
- ☐ Dokumentiertes Datenschutz-Konzept.
- ☐ Umgesetzte Richtlinien zum Datenschutz.

Weitere umgesetzte Maßnahmen / Erläuterungen:

21. Informationssicherheitsüberprüfungen

Es muss regelmäßig überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Hierfür wird der Auftragnehmer regelmäßige Prüfungen durchführen. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Audits / Überprüfungen bei ihm durchzuführen.

Maßnahmen:

- ☐ Regelmäßige Durchführung von internen Audits zu den Themen Datenschutz- und Informationssicherheit.
- ☒ Durchführung von Penetrationstests.

Weitere umgesetzte Maßnahmen / Erläuterungen: