Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Zwischen

nachstehend „Auftraggeber“ genannt

und

ALVARA Digital Solutions GmbH
Querstraße 18
04103 Leipzig

nachstehend „Auftragnehmer“ genannt

Präambel

(1) Der vorliegende Auftragsverarbeitungsvertrag (kurz: „AVV“) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag (kurz „Hauptvertrag“) vom in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

§1 Gegenstand, Dauer und Spezifika der Auftragsverarbeitung

(1) Der AVV kommt mit all seinen Teilen zur Anwendung, sofern und soweit der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) (kurz: „Daten“) verpflichtet hat.

(2) Der AVV bildet den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

(3) Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV und all seiner Teile den Regelungen des zugehörigen Hauptvertrages vor.

(4) Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (kurz: „Spezifika“) werden vor Beginn der Verarbeitung in separaten Anhängen zum AVV (kurz: „AVA“) geregelt. Diese Spezifika sind insbesondere Gegenstand und Dauer sowie Art und Zweck

©02/2022 ALVARA | Digital Solutions

der Verarbeitung, die Kategorie der Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (kurz: „TOM“).

(5) Die AVA sind Bestandteil des AVV. Bei etwaigen Widersprüchen gehen die konkreten Regelungen der AVA der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den AVA auf den AVV Bezug genommen, so ist der AVV mit allen seinen Teilen gemeint.

§2 Verantwortlichkeit und Verarbeitung auf Weisung

(1) Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Der Auftragnehmer handelt ausschließlich weisungsgebunden, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (kurz: „Sperrung“), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer jederzeit ablehnen.

(5) Die Parteien benennen in Textform gegenseitig einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

(6) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen die Weisungen des Auftraggebers kennen und diese beachten.

(7) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

(8) Der Auftragnehmer hat bei der Verarbeitung im Auftrag das Bankgeheimnis zu wahren, soweit der Auftraggeber dem Bankgeheimnis unterworfen ist. Hierauf wird der Auftraggeber den Auftragnehmer hinweisen, sofern dies für den Auftragnehmer aus dem Hauptvertrag nicht ersichtlich ist. Das Bankgeheimnis erstreckt sich auf alle personenbezogenen Daten und anderen Informationen, die dem Auftraggeber über seine Kunden, Interessenten oder über Dritte aus der Geschäftsbeziehung zu diesen bekannt werden. Unter das Bankgeheimnis fällt auch die Angabe, ob der Auftraggeber überhaupt eine Geschäftsbeziehung zu einem Kunden unterhält.

©02/2022 ALVARA | Digital Solutions

§3 Sicherheit der Verarbeitung

(1) Die Parteien vereinbaren technische und organisatorische Maßnahmen (kurz „TOM“) gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten. Diese Maßnahmen sind in den AVA konkretisiert und in Dokumenten dargestellt, die dieser AVV als Anhang beiliegen.

(2) Änderung der vereinbarten TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen

§4 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes von Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht. Mündliche Unterrichtungen sind in Textform nachzureichen. Der Auftragnehmer stimmt sich zur Behandlung solcher Verletzungen mit dem Auftraggeber ab. Die Parteien treffen die erforderlichen Maßnahmen, einschließlich der Maßnahmen zur Minderung möglicher nachteiliger Folgen.

(2) Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu informieren und das weitere Vorgehen mit ihm abzustimmen. Mündliche Unterrichtungen sind unverzüglich in Textform nachzureichen.

§5 Verarbeitungen und Übermittlungen von Daten an einen Empfänger in einem Drittland

(1) Die Verarbeitung von Daten im Auftrag des Auftraggebers findet innerhalb Deutschlands, der EU oder des EWR statt.

(2) Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter den in Art. 44 ff. DSGVO geschriebenen Bedingungen zulässig. Einzelheiten dazu werden in den jeweiligen AVA geregelt.

§6 Unterbeauftragung weiterer Auftragsverarbeiter

(1) Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „Unterauftragnehmer“) erbringen lassen.

(2) Der Auftragnehmer informiert den Auftraggeber rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Die aktuellen Unterauftragnehmer sind der Anlage Spezifika zu entnehmen.

(3) Bei Neubeauftragung oder Änderung von Unterauftragnehmern steht dem Auftraggeber bei Vorliegen eines wichtigen Grundes ein 14-tägiges Widerspruchsrecht zu. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt. Der Widerspruch hat eine Beendigung des Vertrages (ordentliche Kündigung) zur Folge, auf dem die jeweilige AVA basiert.

©02/2022 ALVARA | Digital Solutions

Macht der Auftraggeber keinen Gebrauch von seinem Widerspruchsrecht, gilt das neue Unterauftragsverhältnis als akzeptiert.

(4) Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden technischen und organisatorischen Maßnahmen mindestens dasselbe Schutzniveau aufweisen.

(5) Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

§7 Unterstützung des Auftraggebers bei der Geltendmachung von Betroffenenrechte und bei der Einhaltung seiner Pflichten

Macht eine betroffene Person Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

§8 Kontroll- und Informationsrechte des Auftraggebers

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

(2) Für die Überprüfung der Einhaltung der vereinbarten Schutzmaßnahmen nach § 8.1 und deren geprüfter Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen.

(3) Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017 oder eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Des Weiteren können andere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus § 8.3 bleibt hiervon unberührt.

(4) Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis

©02/2022 ALVARA | Digital Solutions

zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

(5) Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien umzusetzende Maßnahmen ab.

(6) Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich, bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

§9 Haftung und Schadenersatz

(1) Macht ein Betroffener gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

(2) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(3) Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

§10 Laufzeit

(1) Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer AVA wird in der AVA selbst geregelt; ohne eine solche Regelung entspricht die Laufzeit einer AVA derjenigen des AVV.

(2) Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle AVA beendet wurden.

(3) Eine AVA endet mit Beendigung des in der AVA genannten Vertrags, ohne dass es einer gesonderten Kündigung dieser AVA bedarf. Der Auftragnehmer hat in diesem Fall nach Wahl des Auftraggebers die nach der AVA verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform (z. B. durch ein Löschprotokoll) zu bestätigen. Sofern der Auftragnehmer eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen. Entstehen zusätzliche Kosten durch individuelle Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§11 Schlussbestimmungen

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahmung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich in Textform darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

©02/2022 ALVARA | Digital Solutions

(2) Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

(3) Sollte auch nur eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen.

(4) Es gilt deutsches Recht.

Vertragsdatum:

Unterschrift Auftraggeber	Unterschrift Auftragnehmer

©02/2022 ALVARA | Digital Solutions

Anhang zum Auftragsverarbeitungsvertrag

Spezifika Auftragsverarbeitung – ALVARA MünzMarktplatz

Stand: Februar | 2022

§1 Auftraggeber, Auftragnehmer

Auftraggeber/Verantwortlicher	
Auftragnehmer	ALVARA Digital Solutions GmbH Querstraße 18 04103, Leipzig

§2 Allgemeine Einordnung des Anhangs, Gegenstand und Dauer der Verarbeitung

Dieser Anhang zum Auftragsverarbeitungsvertrag (AVA) konkretisiert die allgemeinen Vereinbarungen zur Auftragsdatenverarbeitung wie sie zwischen Auftraggeber und Auftragnehmer im Auftragsverarbeitungsvertrag (AVV) vereinbart wurden. Außerdem enthält diese AVA alle Angaben gemäß DSGVO Art. 30 Abs. 2.

Gegenstand und Dauer sowie Umfang und Art der Verarbeitung ergeben sich aus dem Hauptvertrag vom .

§3 Zwecke der Verarbeitung

Die Verarbeitung der Daten erfolgt im Rahmen des Verkaufs von Kursmünzen in Form von SaaS zu folgenden Zwecken:

- Benutzeranmeldung
- Kontaktaufnahme zur Qualitätssicherung

Formblatt KV 1125 080222

§4 Datenarten, Kategorien betroffener Personen

Art der Daten	Zwecke der Daten	Kreis der Betroffenen
Nachname, Vorname, Zugehörigkeit zum Auftraggeber, E-Mail Adresse	Benutzeranmeldung	Mitarbeiter des Auftraggebers
Nachname, Vorname, Zugehörigkeit zum Auftraggeber, E-Mail-Adresse, Telefonnummer	Kontaktaufnahme zur Qualitätssicherung	Mitarbeiter des Auftraggebers

§5 Erläuterung der Zwecke der Verarbeitung

(1) Benutzeranmeldung:

- Entgegennahme des vom Mitarbeiter des Auftraggebers eingegebenen Benutzernamens (E-Mail-Adresse oder Anmeldekürzels) und Passwortes
- Prüfung auf gültige Anmeldung
- Durchführen aller Nutzeraktionen als dieser angemeldete Benutzer.

(2) Kontaktaufnahme zur Qualitätssicherung:

- Der Auftragnehmer nimmt per Telefon oder E-Mail kontakt mit einem Mitarbeiter des Auftraggebers auf

§6 Unterauftragsverhältnisse

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen
Kupper IT GmbH Prager Str. 15 04013 Leipzig	Rechenzentrumsbetrieb

§7 Übermittlung von Daten an Empfänger in Drittstaaten

Eine Übermittlung von Daten an Empfängern in Drittstaaten oder internationale Organisationen findet nicht statt.

©02/2022 ALVARA | Digital Solutions

§8 Technische und organisatorische Maßnahmen

Im Rahmen des Betriebs der Online-Plattform ALVARA ICC wurden technische und organisatorische Maßnahmen ergriffen wie sie im Anhang „Technische und organisatorische Maßnahmen nach Art. 32 DSGVO, Bereitstellung und Betrieb der Online-Plattform ALVARA MünzMarktplatz“ beschrieben sind.

§9 Kommunikation

Die zuständigen Ansprechpartner sind separat im Kontaktbogen aufgeführt.

©02/2022 ALVARA | Digital Solutions

Technische und organisatorische Maßnahmen nach Art. 32 DGSVO

- ALVARA MünzMarktplatz -

Stand: Januar | 2022

§1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(1) Zutrittskontrolle:

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Empfang [RZ,AN]
- Besucherbuch [RZ]
- Besucherausweis [RZ]
- Persönliche Besucherführung [RZ]
- Zutrittskontrollsystem mit Sicherheitszonen [RZ]
- Zentrales Schließsystem [RZ]
- Sicherheitsschlösser [RZ,AN]
- Personenschleuse mit Vereinzelung [RZ]
- Separat verschlossene Kaltgangeinhausung [RZ]
- Wachschutz mit Anmeldung [RZ]
- Sichtschutz [RZ]
- Videoüberwachung [RZ]
- Transponder [RZ]

(2) Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben

- Nutzerkennung [RZ]
- Passwortwiederholungssperre nach 3 Fehlversuchen [RZ,AN]
- Passwortrichtlinie Komplexität [RZ,AN]
- Passwortrichtlinie Änderungszyklus [RZ]
- Wachdienst [RZ]
- Einsatz von Anti-Viren-Software [RZ,AN]
- Einsatz moderner Firewall-Technologie [RZ,AN]
- Schnittstellenschutz (Netzschaltschränke, Schutz nicht benötigter Netzsteckdosen) [RZ]
- Passwortgeschützter Benutzerzugang [Anwendung]

(3) Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- Verwendung eines Berechtigungskonzepts (Gruppen- und Zugriffsrichtlinien) [RZ,AN]
- Berechtigungsprofile soweit erforderlich differenziert nach Leseberechtigung und Schreibberechtigung [RZ]
- Programmprüfungs- und Freigabeverfahren [RZ]
- Protokollierung und Auswertung von sicherheitskritischen Vorfällen [RZ]
- Mandantenfähigkeit [Anwendung]
- Fachkundige Akten- und Datenvernichtung [RZ,AN]

Formblatt K U 206 080222

(4) Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personen-bezogene Daten getrennt verarbeitet werden.

- Das Host-System ist virtuell von anderen Systemen getrennt [RZ]
- Anwendungsdaten werden in einem eigenen Datenbankschema gehalten [RZ,AN]
- Trennung der Produktions-, Test- und Entwicklungsumgebungen [RZ,AN]
- Eigene Datenbankinstanz je Umgebung. [RZ]
- Trennung der Zugriffsberechtigungen je Systemumgebung [RZ,AN]
- Trennung der Produktions-, Test- und Entwicklungsumgebungen [RZ,AN]

(5) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Daten, die mit Personenbezug erfasst wurden, dienen dazu, gerade diesen Personenbezug herstellen zu können. (z.B. personalisiertes Login)

§2 Integrität (Art. 32 Abs. 1 lit. b. DSGVO)

(1) Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet [RZ,AN]
- Einrichtung von Verschlüsselung (HTTPS, VPN), Firewall [RZ,AN]
- Gekapselte Daten/Systeme [RZ]
- Protokollierung von Datenübermittlungen (Mitschnitt von Fernwartungen) [RZ]
- Verschlüsselung mobiler Datenträger [RZ]
- Sperrung unbefugter Geräte [RZ]
- Sicherheitsrichtlinie für der verschlüsselten Transport [RZ]
- Richtlinie für mobile Endgeräte [RZ]
- Datenvernichtung nach BSI-Standard durch externe Dienstleister mit Vernichtungszertifikat [RZ]

(2) Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- Protokollierung der Benutzung von Datenverarbeitungssystemen [RZ]
- Benutzeridentifikation [Anwendung]
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts [RZ,AN]
- Protokollierung von Nutzeraktionen, Vorhalten der Websession-Verläufe [Anwendung]
- Historisierung von Datenänderungen [Anwendung]

§3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- Redundante Klimasysteme [RZ]
- unterbrechungsfreie Stromversorgung (USV) [RZ]
- mehrere Generatoren [RZ]
- Brandschutz nach VdS [RZ]
- RAS-Systeme [RZ]
- Sauerstoffreduzierung [RZ]
- Separate Brandabschnitte [RZ]
- Sicherungskonzept [RZ]

©02/2022 ALVARA | Digital Solutions

§4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

(1) Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grund-anforderungen genügende Organisation vorhanden ist:

- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit [RZ,AN]
- Bestellung eines Datenschutzbeauftragten [RZ,AN]
- Verpflichtung der Mitarbeiter auf das Datengeheimnis [RZ,AN]
- Hinreichende Schulung der Mitarbeiter in Datenschutzangelegenheiten [RZ,AN]
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO) [AN]
- Durchführen von Datenschutzfolgeabschätzungen. Soweit erforderlich (Art. 35 DSGVO) [AN]

(2) Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO) [AN]
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO) [RZ, AN]

(3) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

- Passwortmindestlänge [Anwendung]
- Benutzeranlage nur mit benötigten Informationen [Anwendung]]

(4) Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) [AN]
- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers [RZ,AN]
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern [RZ,AN]
- Verpflichtung der Mitarbeiter auf das Datengeheimnis [RZ,AN]
- Ticketsystem zur Nachvollziehbarkeit von Anfragen und Servicereaktionen [RZ,AN]

[RZ] : Maßnahmen im Rechenzentrum
[AN] : Maßnahmen beim Auftragnehmer
[Anwendung] : Maßnahmen in der Anwendung

©02/2022 ALVARA | Digital Solutions