Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung zwischen

Auftraggeber/Ihre Organisation
- Im Folgenden Auftraggeber genannt -

und der

rising systems AG
Benrather Schloßallee 99
40597 Düsseldorf
- Im Folgenden der Auftragnehmer genannt -

§ 1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags ist die Bereitstellung einer Instanz der Software ATHLETIQ unter eigener Subdomain und mit eigener Datenbankinstanz. ATHLETIQ stellt dem Auftragnehmer Funktionen zur Organisations- und Talentverwaltung zur Verfügung, zum Beispiel für Athleten, Trainingsräume, Trainer und andere Bereiche.

1.2 Dauer

Der Auftrag ist unbefristet erteilt und gilt solange, wie Leistungen durch den Auftraggeber bezogen werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 2 Konkretisierung des Auftragsinhalts

Einzelheiten zu Art und Zweck der vorgesehenen Verarbeitung oder Nutzung sind unter der „Anlage 1 - Art der personenbezogenen Daten / Kreis der Betroffenen“ zu dieser Vereinbarung aufgeführt. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
Das angemessene Schutzniveau wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c DSGVO).

Die Kategorien der Betroffenen und die Art der personenbezogenen Daten sind in der „Anlage 2 - Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO“ aufgeführt.

§ 3 Technisch-organisatorische Maßnahmen

a) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
b) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 2].
c) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

a) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

a) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
b) Eine Unterbeauftragung ist zulässig.
c) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
d) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
e) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers [mind. Textform]. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Kontrollrechte des Auftraggebers

a) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
b) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
c) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen [z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren];
d) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

a) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
   1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationenunverzüglich zur Verfügung zu stellen
   4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

b) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

a) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

b) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

c) Weisungsberechtigte Personen des Auftraggebers werden in Anlage 3 genannt.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

a) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

b) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

c) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Salvatorische Klausel, Gerichtsstand

a) Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

b) Als Gerichtsstand wird Düsseldorf vereinbart.

Anlage:
Anlage 1 - Art der personenbezogenen Daten / Kreis der Betroffenen
Anlage 2 - Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Anlage 1:

A. Zu § 2 Ergänzungen zu Art und Zweck der Datenverarbeitung
Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung sind:
Der Auftragnehmer bearbeitet Aufträge des Auftraggebers die über das Webinterface aufgegeben werden, sowie der damit im Zusammenhang stehenden Leistungen wie z.B. DNS, Handle-Verwaltung, Webspace, eMailkonten, Unterkonten, Domains etc. Je nach Auftrags-Operation werden zusätzliche personenbezogene Daten wie z.B. Personalausweise, Handelsregisterauszüge zur vollständigen Auftragserfüllung (nach Registry-Bedingungen) benötigt. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler Domainprovider / Registrar im Bereich der Domain-Verwaltung, des Supports bzw. der Verarbeitung von Domain-Aufträgen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Der Auftragnehmer stellt dem Auftraggeber Webhosting-Dienstleistungen bzw. eines (oder mehrerer) dedizierten/dedizierter Server sowie der damit im Zusammenhang stehenden Leistungen wie z.B. EMail, etc. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Produkt und vereinbarten Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, FTP-Servers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen). Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung sind: Der Auftragnehmer bearbeitet Aufträge des Auftraggebers die über das Webinterface aufgegeben werden, sowie der damit im Zusammenhang stehenden Leistungen wie z.B. DNS, Handle-Verwaltung, Webspace, eMailkonten, Unterkonten, Domains etc. Je nach Auftrags-Operation werden zusätzliche personenbezogene Daten wie z.B. Personalausweise, Handelsregisterauszüge zur vollständigen Auftragserfüllung (nach Registry-Bedingungen) benötigt. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler Domainprovider / Registrar im Bereich der Domain-Verwaltung, des Supports bzw. der Verarbeitung von Domain-Aufträgen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Der Auftragnehmer stellt dem Auftraggeber Webhosting-Dienstleistungen bzw. eines (oder mehrerer) dedizierten/dedizierter Server sowie der damit im Zusammenhang stehenden Leistungen wie z.B. EMail, etc. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Produkt und vereinbarten Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, FTP-Servers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen). Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

B. Zu § 2 Art der personenbezogenen Daten
□ – Personenstammdaten
□ - Kommunikationsdaten (z.B. Telefon, E-Mail)
□ - Vertragsstammdaten (Vertragsbeziehung, Produkt-bzw. Vertragsinteresse)
□ – Kundenhistorie
□ - Vertragsabrechnungs- und Zahlungsdaten
□ - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

C. Zu § 2 Kreis der Betroffenen
□ – Kunden
□ – Interessenten
□ – Abonnenten
□ – Beschäftigte
□ – Lieferanten
□ – Handelsvertreter
□ – Ansprechpartner

Anlage 2. Allgemeine technische und organisatorische Maßnahmen (TOMs)
Zum Schutz von personenbezogener Daten gemäß Art. 32 DSGVO Dieses Dokument dient zur Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, vorläufig zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem Auftraggeber bei wesentlichen Änderungen und im Übrigen jährlich zur Durchführung der Auftragskontrolle vorzulegen. Dokumentationen der nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen.

a) Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO: Pseudonymisierung)

Wie wird die Pseudonymisierung der Daten gewährleistet?

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

Regelungen für digitale Pseudonymisierung

- Data Masking
- Hashing

b) Verschlüsselung (Art. 32 Abs. 1 lit. A DSGVO: Verschlüsselung)

Wie wird die Verschlüsselung gewährleistet?

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

Techniken zur Verschlüsselung

- Data Hashing
- Nutzung von kryptografischen Tools
- TLS/SSL-Transportverschlüsselung
- E-Mailverschlüsselung (PGP, S/MIME o.a.)

c) Fähigkeit der Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO: Zutrittskontrolle)

Nur befugte Personen haben Zugang zu den DV-Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

- Festlegung befugter Personen
- Räume sind verschlossen und nur befugte Personen haben einen Schlüssel
- Elektronisch und mechanische Sicherheitssysteme für
- Haupteingangstüren im Bürogebäude
- Dokumentierte Schlüsselvergabe an Mitarbeiter
- Regelung für Firmenfremde • Betriebsfremde Personen haben keinen Zugang zu den DVAnlagen
- Sicherung außerhalb der Arbeitszeit
- Alle Räume mit DV-Anlagen sind verschlossen
- Alarmanlage

d) Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO: Zugangskontrolle)

- Nur befugte Personen können DV-Systeme nutzen.
- Notebooks und Workstations sind verschlüsselt
- Authentifizierung über Benutzername/Passwort
- Interne EDV-Richtlinien für den Umgang mit DV-Systemen
- Verpflichtung auf das Datengeheimnis. Wird von jeden Mitarbeiter durch die Vertraulichkeitsverpflichtungserklärung vertraglich geregelt
- Benutzerberechtigungen werden durch den zuständigen Bereichsleiter bestimmt
- Dokumentation und Verwaltung von Benutzerberechtigung
- Einsatz von 2-Factor Authentifizierung. Wo es möglich ist, wird eine 2-Factor Authentifizierung verwendet
- Vernichtung von Datenträgern wird durch ein zertifiziertes Unternehmen durchgeführt. Die Vernichtung wird protokolliert
- Der administrative Remotezugriff auf die DV-Anlagen ist ausschließlich über ein VPN oder verschlüsselte Verbindungen (z.B. ssh) möglich
- Einsatz diverser Antivirenlösungen
- Einsatz von Hard- und Softwarefirewalls
- zusätzlicher Login für bestimmte sicherheitsrelevante Software
- zu vergebende Passwörter werden durch die schriftlich fixierte Passwortrichtlinie für Mitarbeiter gewährleistet
- die Speicherung erfolgt unter anderem in einer extra verschlüsselten Passwortverwaltungssoftware
- Passwörter werden in regelmäßige Abständen erneuert

Regelungen für analoge Pseudonymisierung
Maschinelle Vernichtung mit mindestens Sicherheitsstufe (DIN 32757-1) 3 bzw. Sicherheitsstufe (DIN 66399) P-3, T-2

e) Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO: Zugriffkontrolle)
Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Regelung der Zugriffsberechtigung

- Rechtevergabe erfolgt durch den IT-Leiter bzw. Beauftragen der Geschäftseinheit
- Least to know Prinzip bei der Vergabe von Berechtigung
- IT prüft die aktuellen Berechtigungen regelmäßig auf Notwendigkeit
- IT prüft regelmäßig die Protokolle auf Verletzungen der Richtlinien, auch automatisiert und stichprobenartig.

Zeitliche Begrenzungen
- Auto-Logout bei allen Systemen
- Bildschirmsperre
- Wo es möglich ist, Sperren nach ungültigen Anmeldeversuchen
- Wo es möglich ist, Zeitverzögertes Antwortverhalten bei Fehlversuchen

f) Integrität (Art. 32 Abs. 1 lit. B DSGVO: 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.

- Festlegung befugter Personen
- Durch die Vergabe entsprechender Rechte
- 4-Augen-Prinzip
- Entwicklung, Administration und Support arbeiten nach dem 4- Augen-Prinzip
- Mobile Datenträger werden in der Regel nicht verwendet, falls doch sind diese verschlüsselt.
- Festplatten werden überwacht, verschlüsselt und ggf. durch verschließbare Festplatteneinschübe gesichert
- Der administrative Remotezugriff auf die DV- Anlagen ist ausschließlich über verschlüsselte Verbindungen möglich (z.B. VPN, ssh, RDP)
- Auswahl der Auftragnehmer erfolgt in der Regel durch die Geschäftsführung
- Aufteilung der Rechte und Pflichten zw. Auftragnehmer und Auftraggeber geschieht über einen AV-Vertrag nach Artikel 28 DSGVO
-

g) Integrität (Art. 32 Abs. 1 lit. B DSGVO: Eingabekontrolle)
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Verpflichtung auf das Datengeheimnis wird von jeden Mitarbeiter durch die Vertraulichkeitsverpflichtungserklärung vertraglich geregelt.
Die Protokollierung von Systemzugriffen auf personenbezogene Daten werden protokolliert.

h) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DSGVO)
Es ist zu gewährleisten, dass Systeme und Dienste die Fähigkeit besitzen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit in Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
- Die Dienstleistungen werden mit Hilfe mehrerer Rechenzentrumsdienstleisters erbracht, welche nach ISO 27001 zertifiziert sind
- Backupdaten werden physikalisch und örtlich getrennt aufbewahrt
- Unterbrechungsfreie Stromversorgung (USV)
- Spiegelung von Festplatten
- Langzeitarchivierung
- Geeignete Räumlichkeiten zur Archivierung

i) Zweckbindungskontrolle (Art. 28 Abs. 3 S. 2 b) DSGVO
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
- Logische Mandantentrennung über die Software
- Daten für unterschiedliche Zwecke werden durch virtualisierte oder hardwareseitige Mechanismen getrennt
-

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

- Verpflichtung auf das Datengeheimnis wird von jeden Mitarbeiter durch die Vertraulichkeitsverpflichtungserklärung vertraglich geregelt
- Protokollierung von Zugriffen auf personenbezogene Daten werden protokolliert
- Die Dienstleistungen werden mit Hilfe mehrerer Rechenzentrumsdienstleisters erbracht, welche nach ISO 27001 zertifiziert sind
- Backupdaten werden physikalisch und örtlich getrennt aufbewahrt
- Logische Mandantentrennung über die Software
- Daten für unterschiedliche Zwecke werden durch virtualisierte oder hardwareseitige Mechanismen getrennt
- Datenschutzfreundliche Voreinstellungen
- Regelmäßige Überprüfung
- Alle zur Datenverarbeitung genutzten Systeme werden in der Regel so datenschutzfreundlich wie möglich benutzt und konfiguriert
- Eine Pseudonymisierung wird so früh wie möglich vorgenommen
- Interne Programmierungsrichtlinien geben Privacy by Default und Privacy by Design verpflichtend vor