Vertrag über die Auftragsverarbeitung personenbezogener Daten

Der nachfolgende Vertrag über die Auftragsverarbeitung (AV-Vertrag) im Sinne des Art. 28 Abs. 3 DSGVO regelt die Verpflichtung der Parteien zur Wahrung des Datenschutzes, insbesondere personenbezogener Daten, im Rahmen der Auftragsverarbeitung. Der Vertrag bezieht sich auf alle Tätigkeiten, die mit dem Vertrag der Parteien über die Nutzung der Plattform www.equify.de in Zusammenhang stehen.

Dem Verantwortlichen (Art. 4 Nr. 7 DSGVO) für die Datenverarbeitung:

[Firma]

[Straße und Hausnummer]

[Postleitzahl und Stadt]

nachfolgend: Auftraggeber

und dem Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO):

Tyclipso GmbH

Grundstraße 1

01326 Dresden

nachfolgend: Auftragnehmer oder Auftragsverarbeiter

- nachfolgend beide auch „Parteien" genannt -

Präambel

Die Tyclipso GmbH (*Auftragsverarbeiter*) ist Anbieter einer zentralen Online-Kollaborationsplattform in Form einer SaaS-Lösung. Der Auftraggeber ist Kunde und Nutzer der durch den Auftragsverarbeiter zur Verfügung gestellten Applikation.

Mit dieser Vereinbarung sollen die datenschutzrechtlichen Rahmenbedingungen und die Anforderungen und Pflichten im Umgang mit personenbezogenen Daten nach den Vorschriften der Verordnung (EU) 2016/679 - Datenschutzgrundverordnung (DSGVO) festgehalten werden.

§ 1 Gegenstand

1) Vertragsbestandteil ist die Nutzung der unter www.equify.de angebotenen Software als Software as a Service.
2) Der jeweilige Nutzer ist Auftraggeber und schließt im Rahmen der Plattformnutzung einen Vertrag mit dem Auftragnehmer (nachfolgend auch „Hauptleistung"). Es ist nicht ausgeschlossen, dass der Auftragnehmer dabei ggf. auch personenbezogene Daten des Auftraggebers im Sinne der Art. 4 Nr. 2 und Art. 28 DSGVO verarbeitet.
3) Die vertraglich vereinbarte Hauptleistung wird ausschließlich in Deutschland oder in einem anderen Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standard-datenschutzklauseln, genehmigte Verhaltensregeln).
4) Sämtliche Anlagen bilden einen integralen Bestandteil dieser Vereinbarung.

§ 2 Dauer

1) Die Laufzeit des Auftragsverarbeitungsvertrages richtet sich nach der Laufzeit der Zusammenarbeit innerhalb des Vertragsgegenstandes der Hauptleistung, sofern sich aus den Bestimmungen des Auftrags-verarbeitungsvertrages nicht darüberhinausgehende (nachvertragliche) Verpflichtungen ergeben
2) Ohne Einhaltung einer Frist kann der Auftraggeber jederzeit den Vertrag kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt,

der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 3 Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

1) Die Verarbeitung personenbezogenen Daten erfolgt ausschließlich zur Erbringung der Hauptleistung durch den Auftragsnehmer.
2) Bei den verarbeiteten Daten handelt es sich um Daten der Projektmitglieder des jeweiligen Projekts und Daten des Auftraggebers. Insbesondere werden folgende personenbezogene Daten der Projektmitglieder verarbeitet:
   - Vorname, Name
   - ggf. Unternehmen/ Organisation/ Verein etc.
   - ggf. Tätigkeit, Abteilung
   - E-Mail-Adresse
   - Benutzername

Von der Datenüberlassung sind keine besonderen personenbezogenen Daten (vgl. Artikel 9 DSGVO) umfasst.

§ 4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§ 5 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

1) Beim Auftraggeber ist – soweit es sich um eine Personengesellschaft oder juristische Person handelt – deren geschäftsführender Gesellschafter bzw. Organ juristischen Person und im Übrigen (bei Einzelunternehmen) der Auftraggeber selbst weisungsberechtigt.

2) Weisungsempfänger beim Auftragnehmer ist ausschließlich dieser selbst. bzw. deren Geschäftsführer. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 6 Pflichten des Auftragnehmers

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen über die Hauptleistung und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Bundesrepublik Deutschland hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
2) Der Auftragnehmer verwendet die vom Auftraggeber zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.
3) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 15 bis 18, 20 und 21 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang gegen Erstattung der dadurch vernunftgemäß beim Auftragnehmer entstehenden Kosten mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO). Der Auftragnehmer hat die dazu erforderlichen Angaben jeweils binnen angemessener Frist an den Auftraggeber weiterzuleiten.
4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden

Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

5) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

§ 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutz- rechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer gewährleistet, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß § 4 dieses Vertrages durchführen.

§ 8 Unterauftragsverhältnisse (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer (vgl. Artikel 28 Abs. 2 S. 2 DSGVO) gestattet, welche ihrerseits das Recht zur Beauftragung von Unterauftragnehmern haben. Der Auftragnehmer wird seine Auftragsverarbeiter in mindestens gleichem Maße wie er selbst in vorliegendem Maße verpflichtet ist, verpflichten.
2) Der Auftragnehmer wird den Auftraggeber über Änderungen, insbesondere die Beauftragung neuer Subunternehmer, informieren.

§ 9 Eigene Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO) des Auftragnehmers

1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
2) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber vor Vertragsschluss abgestimmt worden. Die aktuell vom Auftragnehmer gewährleisteten TOM ergeben sich aus ANHANG 1. Soweit die beim Auftragnehmer getroffenen Maßnahmen im Falle der Mitteilung eines neuen Anforderungsprofils seitens des Auftraggebers etwaig künftig geänderten Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiter-entwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren. Für die Information im Sinne des vorstehenden

Satzes ist die entsprechende Änderung hierüber in mindestens Textform notwendig.

§ 10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

1) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche seitens des Auftraggebers in seinen Besitz gelangte personenbezogene Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen oder dem Auftraggeber auszuhändigen und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 11 Vergütung

1) Die Auftragsverarbeitung wird ohne eine über die Hauptleistungsvergütung hinausgehende Zusatzvergütung vereinbart, soweit nicht vorstehend etwas Anderes geregelt wurde.

§ 12 Haftung

1) Auf Art. 82 DSGVO wird verwiesen, soweit nachfolgend nichts Abweichendes vereinbart wird. Die Parteien vereinbaren für einen etwaigen Innenausgleich des Auftragnehmers gegenüber dem Auftraggeber, dass etwaige zugunsten des Auftragnehmers im Hinblick auf die Hauptleistung dem Grunde oder der Höhe nach vereinbarte Haftungsbeschränkungen auch auf diesen Vertrag Anwendung finden. Wird der Auftragnehmer durch den Betroffenen direkt in Anspruch genommen, so steht ihm zudem über die Regelung des Artikel 82 DSGVO hinaus gegenüber dem Auftraggeber ein vertraglicher Freistellungsanspruch auch dann zu, soweit die Forderung des Betroffenen eine etwaige in Bezug auf die Hauptleistung vereinbarte Haftungsbeschränkung der Höhe nach überschreitet.

§ 13 Informationspflichten, Vorgehen bei Pfändungen Dritter und Insolvenz

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

dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »verantwortlicher Stelle« im Sinne der Datenschutz-Grundverordnung liegen.

§ 14 Sonstige Vereinbarungen

1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
3) Es gilt deutsches Recht.

Anlagen:

- ANHANG I – Technische und Organisatorische Maßnahmen der Tyclipso GmbH
- ANHANG II – Liste der Unterauftragsverarbeiter

ANHANG I – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Verantwortlicher:

Firma:	Tyclipso GmbH
Anschrift:	Grundstraße 1, 01326 Dresden
Telefon:	+49 (0)351 3122303
E-Mail:	tyclipso@ws-datenschutz.de
Internet:	https://www.tyclipso.net

Datenschutzbeauftragter:

Firma:	Kemal Webersohn, LL.M. / Christian Scholtz, LL.M. WS Datenschutz GmbH
Anschrift:	Dircksenstraße 51, 10178 Berlin
Telefon:	030 / 88 72 07 88
E-Mail:	kontakt@ws-datenschutz.de

bestätigt die Einhaltung der nachfolgenden technischen und organisatorischen Maßnahmen zur Datensicherheit nach Art. 32 DSGVO.

Datum der Eintragung: 09.05.2023

1. Organisationskontrolle

Zweck:
Die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Gemeint ist damit, dass sich der Datenschutz nicht an die Organisation, sondern die Organisation an den Datenschutz anpassen sollte.

Maßnahmen:

☒ Mitarbeiter werden regelmäßig (mindestens alle zwei Jahre) auf das Datengeheimnis verpflichtet
☒ Mitarbeiter werden regelmäßig (mindestens einmal jährlich) auf den Datenschutz am Arbeitsplatz sensibilisiert
☒ Es wird regelmäßig eine Auditierung durch den Datenschutzbeauftragten vorgenommen.
☒ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden.
☐ Anmerkungen:

2. Pseudonymisierung gem. Art. 32 Abs. 1 lit. a) DSGVO

Maßnahmen:

☐ Personenbezogene Daten mit normalem Schutzbedarf werden in 2 Teile aufgebrochen und damit pseudonymisiert.
☐ Personenbezogene Daten mit erhöhtem Schutzbedarf werden in 2 Teile aufgebrochen und damit pseudonymisiert.
☐ Es werden, soweit möglich, pseudonymisierte und anonymisierte Daten verwendet
☐ Anmerkungen:

3. Verschlüsselung gem. Art 32 Abs.1 lit. a) DSGVO

Maßnahmen:

☒ Verschlüsselung von Festplatten mit personenbezogenen Daten
☒ Verschlüsselung von Smartphone-Inhalten
☐ Verschlüsselung von mobilen Datenträgern
☐ Verschlüsselung von E-Mails (z.B. PGP)
☐ Anmerkungen:

4. Vertraulichkeit gem. Art 32 Abs.1 lit. b) DSGVO

a) Zutrittskontrolle

Zweck:
Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
☒ Alarmanlage
☐ Automatisches Zutrittskontrollsystem, Ausweisleser
☒ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
☒ Sicherheitsschlösser
☐ Chipkarten-/Transponder-Schließsystem
☐ Biometrie (Fingerabdrücke o. ä.)
☒ Manuelles Schließsystem
☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
☐ Werkschutz/Pförtner
☐ Empfang mit Anmeldung
☐ Sorgfältige Auswahl von Wachpersonal
☒ Sorgfältige Auswahl von Reinigungspersonal
☒ Lichtschranke/Bewegungsmelder
☐ Feuerfeste Türen
☐ Fenstervergitterung
☒ Videoüberwachung der Zugänge
☒ Anmerkungen:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: elektronisches Schlüsselsystem mit protokollierter Ausgabe und Rücknahme, separate Schließgruppen, entsprechend eingerichteten Sicherheitszonen, elektrische Türöffner, Alarmanlage, datenschutzkonforme Perimetrie Überwachung (Videoanlage).

Alle Besucher werden persönlich begleitet.

Es existiert ein geregelter Workflow zur Genehmigung, Verwaltung und Löschung von Zutrittsberechtigungen. Die Geschäftsführung, bzw. deren Beauftragte prüfen periodisch (mind. jährlich) die Notwendigkeit von Zutrittsmedien für die Beschäftigten und veranlassen notwendige Schritte.

IT-Systeme für die öffentliche Bereitstellung von Online-Plattformen werden ausschließlich in gesicherten Rechenzentren von Dritten betrieben.

b) Zugangskontrolle

Zweck:
Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

☒ Authentifikation mit Benutzer + Passwort
☒ Verwaltung von Benutzerberechtigungen
☒ Erstellen von Benutzerprofilen
☒ Einsatz von Anti-Viren-Software
☒ Passwortvergabe / Passwortregeln
☒ Einsatz von Firewalls
☒ Einsatz von VPN-Technologie
☒ Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern
☐ Blickschutzfolien für mobile Rechner
☒ Anmerkungen:

Keine unbefugte Systembenutzung: eindeutige Nutzer-IDs mit sicheren Kennwörtern, IP-Sperre, Verschlüsselung von Datenträgern.

Die lokalen IT-Systeme werden mittels VLANs in separate logische Netze unterteilt.

Weitere technische Absicherungen erfolgen über Firewalls und Proxyserver in den Systemen des Verantwortlichen und der externen Rechenzentren.

Es werden nur verschlüsselte, authentifizierte Verbindungen zum Datentransport genutzt.

c) Zugriffskontrolle

Zweck:
Gewährleistung, 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.

Maßnahmen:

☒ Schriftliches Berechtigungskonzept vorhanden
☒ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
☒ Verwaltung der Rechte durch System-Administrator
☒ Anzahl der Administratoren auf das "Notwendigste" reduziert
☐ Gesicherte Nutzung von USB-Schnittstellen
☒ Automatische Sperrung des Arbeitsplatzes
☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☒ Einsatz von Akten-/Datenträgervernichtern
☒ Verschlüsselung von Datenträgern
☒ Sichere Aufbewahrung von Datenträgern
☒ Ordnungsgemäße Vernichtung von Datenträgern
☒ Löschungskonzept für Daten
☐ Protokollierung der Vernichtung
☒ Anmerkungen:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Jeder Beschäftigte kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.

Alle Beschäftigten des Verantwortlichen werden schriftlich auf das Datengeheimnis (DSGVO) und die Verschwiegenheit verpflichtet.

Nicht benötigte Dienste, Ports und Accounts werden standardmäßig deaktiviert/gesperrt.

d) Trennungskontrolle

Zweck:
Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

Maßnahmen:

☒ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☒ Logische Mandantentrennung (softwareseitig)

☒ Trennung von Produktiv- und Testsystem
☒ Technologie zur Festlegung von Datenbankrechten
☒ Trennung von Daten verschiedener Auftraggeber
☐ Anmerkungen:

e) Weitergabekontrolle

Zweck:
Gewährleistung, 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.

Maßnahmen:

☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
☒ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
☐ E-Mail-Verschlüsselung
☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☐ Protokollierung von Übermittlungen
☒ Anmerkungen:

Grundsätzlich werden personenbezogene Daten nur verschlüsselt oder passwortgeschützt übertragen oder versendet. Verlassen die Daten beim Transport über Dateitransfer das separierte Netz des Verantwortlichen werden zusätzlich SSL/TLS-, IPSec oder VPN-Verbindungen verwendet.

Die Integrität der personenbezogenen Daten bei der Speicherung und Weitergabe innerhalb der DV-Systeme und DV-Anwendungen wird durch Plausibilitätsprüfungen und/ oder Verifizierungsverfahren sichergestellt. Firewall-Systeme und ständig aktualisierte Virensoftware sichern die Kommunikation im Internet.

5. Integrität gem. Art 32 Abs.1 lit. b) DSGVO

a) Eingabekontrolle

Zweck:
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☐ Zentraler Protokoll-/Log-Server
☐ Hash Werte werden erzeugt und zur Überprüfung benutzt
☐ Protokollauswertungsroutinen/-systeme vorhanden
☒ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden
☒ Anmerkungen:

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind: Protokollierung, Dokumentenmanagement.

Durch die strikte Umsetzung des Rollenkonzeptes verfügt jeder Nutzer nur über die Rechte, die er für die Erledigung seiner Arbeitsaufgaben benötigt. Darüber hinaus werden Administratorenzugriffe zusätzlich wie folgt dokumentiert: SSH: Log- und Protokolldaten für Administrator-zugang über Shell.

b) Dokumentationskontrolle

Zweck:
Gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten derart dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

Maßnahmen:

☒ Führung eines Verarbeitungsverzeichnisses
☒ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
☐ Anmerkungen:

c) Auftragskontrolle

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

Maßnahmen:

☒ Vorhandene Vereinbarungen zur Auftragsverarbeitung
☒ Kontrolle der Vertragsausführung
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ Regelung zu Wartungen (speziell Fernwartung)
☒ Zugriffsberechtigte Mitarbeiter sind auf das Datengeheimnis verpflichtet.
☒ Mitarbeiter haben Arbeitsanweisungen/Richtlinien oder Merkblätter erhalten, die über Maßnahmen zur Einhaltung des Datenschutzes sowie der IT-Sicherheit informieren.
☒ Bei Fehlern hinsichtlich der Datenverarbeitung oder Verstoß gegen den Datenschutz erfolgt unverzügliche Information an den Auftraggeber.
☒ Anmerkungen:

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

In den IT-Systemen ist sichergestellt, dass die zur Verfügung gestellten Daten entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben werden. Gleiches gilt für auftragsbezogene Auskünfte; sie werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt.

6. Verfügbarkeitskontrolle gem. Art. 32 Abs. 1 lit. b) DSGVO

Zweck:
Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

☒ Unterbrechungsfreie Stromversorgung (USV)
☒ Überspannungsschutz
☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

☒ Feuer- und Rauchmeldeanlagen
☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☒ Klimaanlage in Serverräumen
☒ Redundante Netzwerktechnik
☒ Schutzsteckdosenleisten in Serverräumen
☒ Feuerlöschgeräte in Serverräumen
☒ Virenschutzsystem
☒ Spiegelung von Festplatten (z. B. RAID-Verfahren)
☐ Festplatten Cluster Storage (z. B. Gluster, Ceph, S2D)
☒ Intrusion-Detection System (z.B. Snort)
☒ Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner Malware-Protection und Firewallsysteme)
☒ Anmerkungen:

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup-Strategie, Patchmanagement; Virenschutz; Firewall.

Wartung und Störungsbehandlung: durch regelmäßige Wartung der Produktionsanlagen besitzen die technischen Anlagen eine hohe Verfügbarkeit. Dies wird durch entsprechende Serviceverträge sichergestellt.

Datenträger-Aufbewahrung: redundante Datenhaltung auf Speichersystemen mittels RAID-Technik; Erstellung von Backups; sichere Auslagerung von Sicherungskopien.

Organisatorische Maßnahmen: Notfallpläne; Durchführung von Notfallübungen.

Notstrom: Wesentliche Systeme sind mit unterbrechungsfreien Stromversorgungen (USV) versehen.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO).

7. Belastbarkeit gem. Art. 32 Abs. 1 lit. b) DSGVO

Zweck:
Gewährleisten, dass die Systeme auch unter unvorhergesehener Last noch arbeiten.

Maßnahmen:

☐ Memory Over commitment disabled
☐ Disk Over commitment disabled
☐ High-Avail Cluster
☐ virtuelle Serverumgebung
☐ Mixed Cloud Anwendung

☐ Festgelegte/Nachvollziehbare Belastungsgrenzwerte
☐ Überwachungssoftware im Einsatz (z.B. Nagios)
☐ automatische Server Alarmmeldungen an verantwortliche Personen
☐ Anmerkungen:

8. Wiederherstellung gem. Art. 32 Abs. 1 lit. c) DSGVO

Zweck:
Gewährleisten, dass nach einer Störung eine Wiederherstellung personenbezogener Daten erfolgen kann.

Maßnahmen:

☐ Backup Konzept
☒ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
☒ Existierende Vollsicherungen der Server
☒ Disaster Recovery Konzept
☒ Testen von Datenwiederherstellungen
☐ Testen von Serverwiederherstellungen
☒ Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
☐ Anmerkungen:

9. Regelmäßige Überprüfung gem. Art. 32 Abs. 1 lit. d) DSGVO

Zweck:
Gewährleisten, dass Verfahren aktuell bleiben, und eingesetzte Techniken dem „Stand der Technik" entsprechen.

Maßnahmen:

☒ Regelmäßige Bewertung eingesetzter Verfahren
☒ Meldepflicht an den DSB von neu eingesetzten Verfahren
☒ Regelmäßige Software Security Updates
☐ Penetrationstests werden durchgeführt und dokumentiert
☒ Regeln zur Hardwarebeschaffung
☐ Anmerkungen:

ANHANG II – LISTE DER UNTERAUFTRAGSVERARBEITER

Die Unterauftragsverarbeiter werden vom Verantwortlichen beauftragt. Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter angezeigt:

Firma	Anschrift	Kontakt	Funktion
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	IONOS SE, Der Datenschutzbeauftragte Elgendorfer Straße 57 56410 Montabaur oder per E-Mail an datenschutz@ionos.de	Hosting