Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO

Präambel

Bestandteil der im Einzelauftrag geregelten Leistungserbringung durch Retarus (nachfolgend: „Auftragnehmer“) für den Kunden (nachfolgend: „Auftraggeber“) ist auch die Verarbeitung von personenbezogenen Daten. Die Regelungen dieser Auftragsverarbeitungsvereinbarung (nachfolgend: „AVV“) finden auf die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer im Rahmen seiner Leistungserbringung Anwendung und konkretisieren insoweit die datenschutzrechtlichen Verpflichtungen der Parteien.

1. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags zum Datenumgang ist die Erbringung der Leistungen gemäß Leistungsbeschreibung des Einzelauftrags.

(2) Die Dauer des Auftrags zum Datenumgang (Laufzeit) entspricht der Laufzeit des Einzelauftrags.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Aufgaben des Auftragnehmers liegen in der Erbringung von Kommunikationsdienstleistungen, wie in der Leistungsbeschreibung des Einzelauftrags näher geregelt.

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. Die Zustimmung kann vom Auftraggeber nicht unbillig verweigert werden.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien:

☒ Personenstammdaten

☒ Kommunikationsdaten (z. B. Telefon, E-Mail, Fax)

☐ Vertragsstammdaten

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ _____

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Empfänger und Versender von Nachrichten, die an den Auftraggeber gerichtet sind oder von diesem ausgehen

☒ Mitarbeiter / Ansprechpartner

☐ Kunden

☐ Lieferanten

☐ Geschäftsleitung

☐ _____

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer wird technische und organisatorische Maßnahmen i.S.v. Art. 32 DSGVO zum angemessenen Schutz der Daten des Auftraggebers treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. (Einzelheiten im Anhang zu dieser AVV).

(2) 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. Betroffenenrechte

(1) 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 oder mit einer Bitte um Auskunft unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer wird den Auftraggeber auf dessen Weisung hin in angemessenem Umfang bei der Umsetzung seines Löschkonzepts sowie der Bearbeitung von Anfragen von Betroffenen bzgl. deren Rechte wie z. B. Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft unterstützen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer ist zur Einhaltung der nachfolgend aufgeführten Vorgaben verpflichtet:

a) Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 f. DSGVO ausübt.

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt, der unter E-Mail

datenschutz@retarus.de

zu erreichen ist. Weitere jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Regelmäßige Kontrolle der internen Prozesse sowie der technischen und organisatorischen Maßnahmen gemäß Ziff. 3, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

c) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung des Auftraggebers zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

d) Sollten die Daten des Auftraggebers beim Auftragnehmer 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 darüber zu informieren. 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“ im Sinne der DSGVO liegen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Ziff. 6 sind Beauftragungen von solchen 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 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 Schutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Einsatz von Unterauftragnehmern (weitere Auftragsverarbeiter) ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat. Der Auftraggeber darf die Zustimmung nicht ohne wichtigen datenschutzrechtlichen Grund verweigern.

(3) Die Zustimmung des Auftraggebers zur Beauftragung eines Unterauftragnehmers gilt als erteilt, sofern der Auftragnehmer dem Auftraggeber die geplante Beauftragung eines Unterauftragnehmers schriftlich oder in Textform angezeigt hat und der Auftraggeber nicht innerhalb von 14 Kalendertagen nach Zugang der Mitteilung schriftlich oder in Textform Einspruch gegen die jeweilige Beauftragung erhoben hat.

(4) Verweigert der Auftraggeber die Zustimmung zu einer vom Auftragnehmer geplanten Unterbeauftragung ohne wichtigen datenschutzrechtlichen Grund, ist der Auftragnehmer berechtigt, den Einzelauftrag unter Beachtung einer angemessenen Auslauffrist zu kündigen. Sofern im Einzelauftrag unterschiedliche Leistungen vereinbart sind, die voneinander trennbar sind und vom Auftraggeber unabhängig voneinander nutzbar sind, gilt das Kündigungsrecht nur für die Teile des Einzelauftrags, die von der Verweigerung der Unterbeauftragung betroffen sind.

(5) Die angemessene Auslauffrist für eine Kündigung gemäß vorstehendem Abs. 4 beträgt maximal sechs (6) Monate oder die Restlaufzeit des Einzelauftrags, je nachdem, welche Frist kürzer ist.

(6) Der Auftraggeber stimmt bereits jetzt der Beauftragung des nachfolgend aufgeführten Unterauftragnehmers zu:

- retarus GmbH, Aschauer Straße 30, 81549 München, Deutschland

(7) Soweit Leistungen im Bereich EDI und/oder OCR Gegenstand des Einzelauftrags sind, stimmt der Auftraggeber bereits jetzt der Beauftragung der nachfolgend aufgeführten Unterauftragnehmer zu:

- Ametras Documents GmbH, Salbeiweg 1, 88436 Eberhardzell, Deutschland
- retarus (Romania) S.R.L., Piața Consiliul Europei, Nr. 2A, United Business Center 1, Sp. U1P3, 300627 Timisoara, Rumänien

(8) Soweit Leistungen im Bereich E-Mail Security Gegenstand des Einzelauftrags sind, stimmt der Auftraggeber bereits jetzt der Beauftragung des nachfolgend aufgeführten Unterauftragnehmers zu:

- Bitdefender S.R.L., Orhideea Towers Building, 15A Orhideelor Avenue, 6th District, 060071 Bukarest, Rumänien

(9) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser AVV dem Unterauftragnehmer im Wege einer Vereinbarung gemäß Art. 28 Abs. 2-4 DSGVO aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten des Auftragnehmers mit geeigneten Mitteln nach, insbesondere durch Zurverfügungstellung der jeweils erforderlichen Informationen.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 10 Kalendertage) durchgeführt. Der Auftragnehmer darf die Durchführung der Inspektion von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Inspektion auch nach Anmeldung mit angemessen verkürzter Vorlaufzeit vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer ist jedoch auch hierbei weitestgehend zu vermeiden.

(4) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Abs. 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

(5) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

8. Mitteilungs- bzw. Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 33 bis 36 DSGVO genannten Pflichten. Hierzu gehören insbesondere:

- die unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Auftraggeber;
- die Unterstützung des Auftraggebers im Rahmen seiner Informationspflicht gegenüber Betroffenen. In diesem Zusammenhang stellt der Auftragnehmer dem Auftraggeber unverzüglich alle relevanten Informationen zur Verfügung;
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9. Weisungsbefugnis und Hinweispflicht des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) 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 Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) 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 Aufbewahrungsfristen erforderlich sind.

(2) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Einzelauftrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) 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. Kostentragung

(1) Sofern der Auftragnehmer den Auftraggeber auf dessen Weisung bei der Einhaltung der in den Artikeln 33 bis 36 DSGVO genannten Pflichten unterstützt (vgl. Ziff. 8 dieser AVV) oder Leistungen gemäß Ziff. 4 dieser AVV erbringt, kann der Auftragnehmer hierfür eine Vergütung unter Zugrundelegung der jeweils gültigen Stundensätze für Beratungs- und Supportleistungen verlangen. Dies gilt nicht, sofern die jeweiligen Leistungen infolge eines Verstoßes des Auftragnehmers gegen seine vertraglichen Pflichten erforderlich geworden sind.

(2) Für die Unterstützung bei der Durchführung einer Inspektion gemäß Ziff. 7 dieser AVV kann der Auftragnehmer eine Vergütung nach Maßgabe der jeweils gültigen Stundensätze für Beratungs- und Supportleistungen verlangen, wenn und soweit die Unterstützung einen Aufwand von mehr als einem Manntag pro Kalenderjahr erfordert.

12. Erweiterung / Schweizer Bundesgesetz über den Datenschutz (DSG)

Die nachstehenden Bestimmungen ergänzen diese Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO zwischen Auftragnehmer und Auftraggeber wie folgt:

1. Für die auftragsbezogene Bearbeitung personenbezogener Daten zwischen Auftragnehmer und Auftraggeber ist, entsprechend dem Territorialitätsprinzip, zusätzlich auch das Schweizer Bundesgesetz über den Datenschutz (DSG) anwendbar.

2. Die Bestimmungen dieser Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO gelten analog auch für die auftragsbezogenen Datenbearbeitungen zwischen Auftragnehmer und Auftraggeber im Anwendungsbereich des DSG.

3. Die auftragsbezogenen Datenbearbeitungen zwischen Auftragnehmer und Auftraggeber im Anwendungsbereich des DSG unterstehen der datenschutzrechtlichen Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

13. Schlussbestimmungen

(1) Soweit zwischen den Parteien bereits Einzelaufträge über die Erbringung von Leistungen durch den Auftragnehmer für den Auftraggeber bestehen, die noch keine Vereinbarungen zur Auftragsverarbeitung nach Maßgabe der DSGVO beinhalten, so gelten die Regelungen dieser AVV entsprechend auch für diese bereits bestehenden Einzelaufträge.

(2) Die Regelungen dieser AVV gelten entsprechend auch für alle etwaigen künftigen Einzelaufträge über die Erbringung von Leistungen durch den Auftragnehmer für den Auftraggeber, soweit in dem jeweiligen Vertrag nicht etwas Abweichendes geregelt ist.

(3) Sollte eine Bestimmung dieser AVV unwirksam oder nicht durchsetzbar sein oder werden oder sollte diese AVV eine Lücke aufweisen, so berührt dies die Wirksamkeit und Durchsetzbarkeit der übrigen Bestimmungen dieser AVV nicht. Die Parteien verpflichten sich für diesen Fall, anstelle der betreffenden unwirksamen Bestimmung oder zur Ausfüllung der Lücke diejenige wirksame und/oder durchsetzbare Bestimmung zu vereinbaren, die dem wirtschaftlichen Zweck dieser AVV am nächsten kommt.

(4) Sofern zwischen den Regelungen dieser AVV und den sonstigen Regelungen des Einzelauftrags Widersprüche bestehen sollten, haben die Regelungen dieser AVV Vorrang vor den sonstigen Regelungen des Einzelauftrags.

(5) Änderungen und Ergänzungen dieser AVV bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Anhang Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

retarus

Anlage

zur Ergänzungsvereinbarung „Auftragsverarbeitung gemäß Art. 28 DSGVO“

Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO

Stand des Dokuments: V4.0 vom 25.07.2025

Präambel:

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Tätigkeit für den Auftraggeber vom Auftragnehmer zu treffenden technischen und organisatorischen Einzelmaßnahmen gemäß Art. 32 DSGVO.

Die Ausführungen zu Rechenzentren beziehen sich auf die aktuellen Standorte der Datenverarbeitung und gelten als Standard für alle etwaigen zukünftigen Einrichtungen.

Dieses Dokument beinhaltet folgende Kapitel:

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) 2
1. Zutrittskontrolle 2
2. Zugangskontrolle 3
3. Zugriffskontrolle 3
4. Trennungskontrolle 4
5. Verschlüsselung 4
II. Integrität (Art. 32 Abs. 1 lit. b DSGVO) 5
1. Weitergabekontrolle 5
2. Eingabekontrolle 5
III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) 6
1. Verfügbarkeitskontrolle 6
IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO) 8
1. Auftragskontrolle 8
2. Management-Systeme 8
V. Änderungsverzeichnis 10

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Zutrittskontrolle

Maßnahmen zum Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen.

1.1 Physische Sicherheit der Rechenzentren

a) Auswahl von professionellen Rechenzentrumsbetreibern mit auditierten Sicherheitsmaßnahmen nach einschlägigen Standards wie ISO/IEC 27001, SOC1, etc.
b) Betrieb der Retarus Infrastruktur in eigenem abgeschlossenem Bereich (z.B. Rack-Cage, etc.) mit strikter Zutrittskontrolle
c) Dokumentiertes Gebäudesicherheitskonzept mit definierten Sicherheitszonen durch den Betreiber
d) Elektronisches Zutrittskontrollsystem mit Protokollierung der Zutritte
e) Zutritt durch Chipkarte in Kombination mit biometrischen Merkmalen (Fingerabdruck oder Handvenen)
f) Vereinzelungsanlagen bei Wechsel von Sicherheitszonen
g) Flächendeckende Videoüberwachung mit min. 90 Tage Vorhaltezeit der Aufnahmen
h) Umzäunung des Geländes
i) Sicherheitspersonal vor Ort mit 24/7 Besetzung
j) Alarmanlage mit Verbindung zu Sicherheitspersonal

1.2 Physische Sicherheit der Bürogebäude

a) Dokumentiertes Gebäudesicherheitskonzept mit definierten Sicherheitszonen
b) Elektronisches Zutrittskontrollsystem mit Protokollierung der Zutritte
c) Zutritt durch Chipkarte
d) Prozess zur Vergabe von Zutrittsmedien und Schlüsseln inkl. Protokollierung
e) Videoüberwachung der Eingangstüren außerhalb der Geschäftszeiten
f) Anweisungen zur Schließregelung

1.3 Organisatorische Zutrittskontrolle

a) Prozesse für Vergabe, Verwaltung, Entzug und Überprüfung von Zutrittsberechtigungen
b) Regelungen bei Verlust/Diebstahl von Zutrittsmedien
c) Richtlinien für Besucher und Betriebsfremde (Anmeldung und Begleitung)
d) Aufsicht von Wartungs- und Reinigungspersonal
e) Sorgfältige Auswahl des Fremdpersonals und namentliche Vergabe von Zutrittsberechtigungen

2. Zugangskontrolle

Maßnahmen zur Verhinderung von unbefugter Systembenutzung.

2.1 Regelung der Zugangsberechtigungen

a) Prozesse für die Vergabe, Verwaltung, den Entzug und die Überprüfung von Zugangsberechtigungen
b) Regelmäßige Überprüfung der Zugangsberechtigungen
c) Einsatz von personalisierten Benutzerkennungen
d) Zentrale Verwaltung von administrativen Notfallbenutzern (Breaking-Glass)
e) Passwort Richtlinie regelt den Umgang mit Passwörtern
f) Etablierte Prozesse zur Rücksetzung von Passwörtern (Verlust oder Vergessen)
g) Automatische Sperrung des Desktops beim Verlassen des Arbeitsplatzes
h) Begrenzung von fehlerhaften Anmeldeversuchen mit anschließender Sperrung bei Überschreitung
i) Zeitliche Befristung bei temporären Zugangsberechtigungen
j) Protokollierung der Benutzung von Zugängen inkl. fehlgeschlagenen Anmeldeversuchen

2.2 Netzwerksicherheit

a) Strikte Trennung der Netzwerke und Zonen wie Produktion, Büro und Gäste (DMZ, VLAN)
b) Absicherung des Zugangs zu den Netzwerken (NAC mittels 802.1x, Enterprise WPA, Radius)
c) Schutz des Netzwerkes durch den Einsatz von Firewalls, Endpoint Protection und Intrusion Prevention Systemen (IPS)
d) Vorgaben zur Härtung und Inbetriebnahme von Netzwerkgeräten inkl. regelmäßiger Kontrolle der Einhaltung
e) Regelungen für die Fernadministration und Fernwartung
f) Fernzugriffe ausschließlich per VPN mit 2-Faktor-Authentifizierung

3. Zugriffskontrolle

Maßnahmen gegen unbefugtes Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten innerhalb des Systems.

3.1 Berechtigungskonzept

a) Regelungen für Vergabe, Verwaltung, Entzug und Überprüfung von Zugriffsberechtigungen
b) Servicebezogene Definition des Berechtigungsmanagement für Eingabe, Kenntnisnahme, Veränderung und Löschung gespeicherter Daten
c) Rollenbasierte Vergabe von Berechtigungen
d) Protokollierte Vergabe/Änderung von Zugriffsberechtigungen

3.2 Zugriffsschutz

a) Systemseitige Trennung von Entwicklung, Test und Produktion

b) Restriktiver Einsatz von SQL
c) Einschränkung der Erlaubnis zur Anwendung von Hilfsprogrammen bzw. Funktionen, die geeignet sind, Sicherheitsmaßnahmen zu umgehen
d) Regelungen für die Datenhaltung (Aufbewahrungsfristen, Löschung, Schutzbedarf)
e) Automatisierte Löschung gemäß den definierten Vorhaltezeiten

3.3 Verwendung und Verwaltung von Datenträgern

a) Regelungen zur gesicherten Datenträgeraufbewahrung in Abhängigkeit vom Schutzbedarf
b) Festlegung der zur Datenträgerentnahme befugten Rollen
c) Regelung der Anfertigung/Ausgabe von Kopien und Duplikaten
d) Prozesse zur sicheren Vernichtung von Datenträgern in Abhängigkeit des Schutzbedarfs

4. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung von personenbezogenen Daten, die zu unterschiedlichen Zwecken erhoben wurden.

4.1 Mandantentrennung

a) Logische Trennung der Mandanten und der jeweiligen Daten
b) Zweckbindung der Daten und Berechtigungen

4.2 Weitere Maßnahmen

a) Innerbetriebliche Vorgaben für die Erhebung und Verarbeitung von Daten
b) Funktionstrennung der Systeme (Entwicklung, Test, Produktion)
c) Dokumentation der Verarbeitungen, Systeme und Datenerhebungszwecke
d) Verzicht auf integrierte Datenspeicherung

5. Verschlüsselung

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

5.1 Allgemein

a) Richtlinie zum Einsatz geeigneter Verschlüsselungsroutinen gemäß des Schutzbedarfs
b) Etablierte Prozesse zur Schlüsselverwaltung

5.2 Technische Maßnahmen

a) Verschlüsselung nach Stand der Technik mit Verfahren wie etwa AES, RSA, Elliptic Curve (EC)
b) Verwendung moderner Hashfunktionen für Signaturen wie etwa SHA-256, SHA-3
c) Passwortspeicherung mittels anerkannter Hash Methoden (Salted-Hash)
d) Verschlüsselte Datenübertragung von/aus externen Netzen mittels geeigneter Transportprotokollen (TLS, SSH, S/MIME, PGP)
e) Verschlüsselte Datenträger in mobilen Geräten
f) Bei Langzeitspeicherung (Archiv) Verschlüsselung auf Dateiebene

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1. Weitergabekontrolle

Maßnahmen zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten bei elektronischer Übertragung oder Transport.

1.1 Sicherheit bei der Datenübertragung

a) Verschlüsselte Datenübertragung von/aus externen Netzen mittels geeigneter Transportprotokollen (TLS, SSH, S/MIME, PGP)
b) Verwendung von elektronischen Signaturen (bei Emails)
c) Festlegung der Übermittlungswege, Protokolle und der Datenempfänger
d) Protokollierung der Datenübermittlung

1.2 Sicherer Umgang mit Datenträgern

Die Ausführungen unter Ziff. I.3.3 gelten auch an dieser Stelle. Zusätzlich gilt:

a) Regelungen für einen sicheren Transport von Datenträgern definiert
b) Transport von Datenträgern mit personenbezogenen Daten ist nicht vorgesehen
c) Etablierte technische Einschränkungen zur Benutzung von USB-Wechseldatenträgern

2. Eingabekontrolle

Maßnahmen zur Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

2.1 Protokollierung und Zugriffe

a) Konzept zur Protokollierung von Benutzeraktivitäten, technischen Systemereignissen, Fehlern und sicherheitsrelevanten Aktivitäten
b) Berechtigungskonzept berücksichtigt Rechte für unterschiedliche Zwecke (lesen, schreiben, löschen)
c) Verwendung von individuellen Benutzerkennungen
d) Zentrale Speicherung der relevanten Logs mit besonderen Anforderungen an die Zugriffsrechte

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

1. Verfügbarkeitskontrolle

Maßnahmen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von personenbezogenen Daten.

1.1 Backup von Daten

a) Allgemeines Konzept und Richtlinien für eine Datensicherung
b) Mindestens tägliche verschlüsselte Sicherung von Konfigurationsdaten und Datenbanken
c) Kennzeichnung von Datenträgern bei Lagerung (Archivierung)
d) Bestandskontrolle von Datenträgern
e) Protokollierung von Datenbackups und Rücksicherungen
f) Lagerung der Backups von kritischen Systemen in einem anderen Brandabschnitt oder einem anderen Standort
g) Ausreichende Aufbewahrungsdauer von Sicherungsdaten
h) Regelmäßige Integritätstest und Rücksicherungstest von Backups

1.2 Sicherer Betrieb in den Rechenzentren

a) Unterbrechungsfreie Stromversorgung

- Redundante USV-Anlage mit Notstromaggregat
- Netzersatzanlage mit ausreichendem Treibstoffvorrat und SLA für Treibstoffnachlieferung
- Regelmäßige Wartung und Tests der Notstromversorgung

b) Brandschutz und Brandvermeidung

- Brandmeldeanlage mit Brandfrüherkennung
- Löschung mittels Löschgasanlage (z.B. Inert, Argon)
- Direkte Aufschaltung zur örtlichen Feuerwehr
- Brandschutzabschnitte mit min. Feuerwiderstandsklasse F90
- Regelmäßige Wartung der gesamten Anlage

c) Klimatisierung

- Redundante Klimatisierungssysteme (CRAC)
- Trennung von Kalt- und Warmbereich
- Permanentes Monitoring der Temperaturen
- Regelmäßige Wartung der gesamten Anlage

d) Internetanbindung und Telefonie

- Mehrfachredundante und Carrier-neutrale Internetanbindung

- Direkter Zugang zu allen wichtigen Carriern und redundante Anbindung an alle wichtigen Peering Punkte (CIX enabled site)
- Anbindung des Retarus Netzwerks an min. zwei verschiedene Carrier
- Eigene produktspezifische Lastverteilung
- SLA mit 24x7 Servicevereinbarungen
- Schutzmaßnahmen gegen DDoS Angriffe

1.3 Bereitstellung und Betrieb durch Retarus

a) Erlass und zentrale Verwaltung von Sicherheitsrichtlinien und Dienstanweisungen (SOP)
b) Formalisierte Freigabeverfahren für Inbetriebnahme und Änderungen (Change-Management)
c) Assetmanagement von allen eingesetzten Komponenten (CMDB)
d) Zentrales Konfigurationsmanagement und Einsatz von Werkzeugen zur Orchestrierung von Systemen
e) Permanentes aktives Monitoring der Systeme (24x7x365)
f) Retarus interne Rufbereitschaften zur Entstörung
g) Redundanz durch Clusterbetrieb von allen relevanten Systemen gemäß der Risikobeurteilung
h) Ersatzgeräte von wichtigen Systemen auf Lager

1.4 Maßnahmen zum Notfall- und Katastrophenschutz

a) Dokumentierte Notfall- und Katastrophenplanung im Rahmen des Business Continuity Management
b) Eindeutige Verantwortlichkeiten für die Aktivierung des Emergency Boards
c) Bestehende Richtlinien für Business Continuity (BCM-Plan), Disaster Recovery (DR-Plan) und Pandemic Preparedness (PP-Plan)
d) Regelmäßige Überprüfung und Tests der Notfallpläne
e) Angemessene Schulung der betroffenen Mitarbeiter in der Anwendung des Notfallkonzepts

1.5 Weitere Maßnahmen

a) Vertretungsregelungen
b) Zentrale und einheitliche Beschaffung von Hard- und Software
c) Freigabeprozesse für Software von Drittherstellern
d) Wartungsverträge und SLAs bei Einsatz von Dienstleistern

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

1. Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers.

1.1 Vertragsgestaltung

a) Es besteht eine schriftliche oder zumindest in einem elektronischen Format abgeschlossene Vereinbarung zur Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer
b) Der Auftraggeber erteilt dem Auftragnehmer die Weisungen mindestens in Textform bzw. bestätigt etwaige mündlich erteilte Weisungen unverzüglich mindestens in Textform
c) Der Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers

1.2 Unterbeauftragung

a) Ausreichende Maßnahmen zur Einhaltung des Datenschutzes durch einen möglichen Unterauftragnehmer können auch durch den Auftraggeber geprüft werden
b) Dienstleisterverzeichnis

1.3 Aufsichtsbehörden

a) Im Falle einer Prüfung des Auftragnehmers durch die Aufsichtsbehörde, kann der Auftraggeber den Prüfbericht verlangen
b) Der Punkt a) findet auch bei Prüfungen von möglichen Unterauftragnehmern Anwendung

2. Management-Systeme

2.1 Datenschutz-Management

a) Dokumentierte Prozesse für die Meldung von Datenschutzvorfällen und die Bearbeitung von Betroffenenanfragen
b) Prozess zur datenschutzrechtlichen Prüfung neuer Datenverarbeitungsverfahren
c) Bestellter Datenschutzbeauftragter
d) Verpflichtung von Mitarbeitern auf Geheimhaltung und Datenschutz
e) Verarbeitungsverzeichnis

2.2 Informationssicherheitsmanagement

a) Betrieb eines zertifizierten Informationssicherheit Management Systems (ISMS) nach ISO/IEC 27001
b) Ernennung eines Informationssicherheitsbeauftragten

2.3 Incident-Response-Management

a) Regelungen für den Umgang mit Datenschutz- und Sicherheitsvorfällen
b) Regelungen für Anfragen von Betroffenen

2.4 Change-Management

a) Änderungen an Systemen unterliegen dem zentralen Change-Management Prozess
b) Umsetzung eines Mehr-Augen-Prinzips bei Änderungen (Change Advisory Board)

2.5 Patch Management

a) Regelmäßige Aktualisierung von Betriebssystemen und Applikationen
b) Automatisierte Routinen zur Erkennung von Patch Bedarf und dem Durchführen von Updates

2.6 Regelmäßige Überprüfung

a) Jährliche externe Auditierung des internen Kontrollsystems und ISMS nach ISAE 3402 (SOC1), ISAE 3000 (SOC2), ISO/IEC 27001 und weiteren einschlägigen Zertifizierungen
b) Regelmäßige interne Überprüfungen und Audits durch IT Compliance Abteilung
c) Regelmäßige Schwachstellen Scans (Vulnerability Monitoring)
d) Regelmäßige externe PEN-Tests zur Überprüfung der Netzwerk- und Anwendungssicherheit

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

Es wird durch entsprechende Voreinstellungen bzw. Maßnahmen sichergestellt, dass nur personenbezogene Daten gemäß dem jeweiligen bestimmten Verarbeitungszweck verarbeitet werden. Dies bezieht sich auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Dies wird unter anderem realisiert durch folgende Maßnahmen:

a) Design der Dienste nach „Deliver & Delete“ Prinzip
b) Automatische Löschroutinen
c) Anwendung von Privacy-by-Design Prinzipien

V. Änderungsverzeichnis

Version	Datum	Änderung	Bearbeiter
V3.0	07.03.2018	Neugestaltung des Dokuments wegen Umsetzung DSGVO, alle vorherigen Änderungen wurden aus der Historie gelöscht	Philipp Deml
V3.1	18.02.2021	Überarbeitung und leichte Änderungen an der Formatierung Erweiterung des Maßnahmenkatalogs Kapitel I: 1.5 d), 2.1 a), 2.2 b), 3.2 f) Kapitel III: 1.2 f) g), 1.3 d), 1.4 b) j) k), 1.5 Kapitel IV: 2.3, 2.4, 2.5	Philipp Deml
V.3.1	24.02.2022	Review; Keine Änderungen	Philipp Deml
V.3.1	22.02.2023	Review; Keine Änderungen	Philipp Deml
V.3.1	26.02.2024	Review; Keine Änderungen	Philipp Deml
V4.0	25.07.2025	Auslagerung des Rechenzentrumbetriebs (Colocation Provider), Überarbeitung und Anpassung der Formulierung aller Maßnahmen an den Stand-der-Technik, zusammenfassen oder löschen von betroffenen Punkten. Ergänzung um Kapitel IV, 2.7, Aufnahme der ISO/IEC 27001 Zertifizierung.	Philipp Deml