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) 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

(7) 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

(8) 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. 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

Anhang

zur Anlage „Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO“

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Stand des Dokuments: V3.1 vom 18.02.2021

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 zum Rechenzentrum beziehen sich auf den Hauptstandort Aschauer Str. 30 in 81549 München und stehen exemplarisch für alle Rechenzentren des Auftragnehmers sowie gelten als Standard für alle etwaigen zukünftigen.

Dieses Dokument beinhaltet folgende Kapitel:

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

1. Zutrittskontrolle

Maßnahmen zum Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen.

1.1 Objektsicherung (Rechenzentrum)

a) Eigener Sicherheitsbereich, Zutritt zum Rechenzentrum gesichert durch Zutrittskontrollsystem mit Chipkarten
b) Türsicherung (Magnetschlösser, Ausweisleser und Protokollierung der Zutritte)
c) Kameraüberwachung mit ständiger Aufzeichnung
d) Einbruchmeldesystem/Alarmanlage – siehe Ziff. I.1.7
e) Keine Außenfenster im Rechenzentrum
f) Schächte (Klimaanlage, Umluftanlage, Aufzug, usw.) gesichert
g) Sicherung der Notausgänge gegen missbräuchliche Benutzung – Alarmauslösung durch Fluchttürsteuerungen im UG

1.2 Objektsicherung (Gebäude und Büro)

a) Zutritt zu den Büros durch Zutrittskontrollsystem mit Chipkarten
b) Türsicherung (Motorschlösser, Ausweisleser und Protokollierung der Zutritte)
c) Videoüberwachung der Eingangstüren nach Ende der Bürozeiten
d) Schutz der Außenhaut durch Bewegungsmelder im Treppenhausbereich

1.3 Sicherheitszonen

a) Das Rechenzentrum ist ein getrennter Bereich mit strikter Zutrittsbeschränkung und Überwachung
b) Die für die Administration der Dienste zuständigen Bereiche wie Operation, Network und Application Management sind räumlich zusammengefasst, abgetrennt und mit einer zusätzlichen Zutrittskontrolle versehen

1.4 Organisatorische Zutrittskontrolle

a) Kontrollgänge durch Sicherheitsdienst nach Ende der Bürozeiten
b) Schlüsselregelung
c) Schließregelung (Türen und Fenster sind immer geschlossen zu halten, Alarmanlage im Rechenzentrum bei Abwesenheit immer scharf geschaltet)
d) Kennzeichnung der Notausgänge und Fluchtwege

1.5 Regelung der Zutrittsberechtigungen

(im Folgenden bezogen auf das Rechenzentrum)

a) Zutrittsregelungen für Personen und Personengruppen (Mitarbeiter, Führungskräfte, Firmenfremde, Besucher, Wartungs-, Reinigungspersonal, Lieferanten, Boten, usw.)
b) Regelung beim Ausscheiden und Wechseln von Berechtigten
c) Regelungen/Folgemaßnahmen bei Verlust von Ausweisen, Schlüsseln, usw.
d) Besucherregelung inkl. Verpflichtung auf Einhaltung des Datenschutzes bei Zutritt
e) Anmeldung und Begleitung von Besuchern und Firmenfremden
f) Aufsicht des Wartungs-, Reparatur- und Reinigungspersonals
g) Revisionsfähige Vergabe und Entzug der Zutrittsberechtigungen

1.6 Personenkontrolle

a) Kontrolle des Betriebspersonals
b) Kontrolle des Wartungs-, Reparatur-, und Reinigungspersonals
c) Kontrolle von Besuchern

1.7 Alarmanlage

a) Gefahrenmeldeanlage zertifiziert nach VDS
b) Unscharfschaltung nur durch per Chipkarte autorisiertes Personal mit zusätzlicher Codeeingabe
c) Unscharfschaltung (Scharfschaltung „vergessen“) außerhalb der Kernzeiten löst einen Alarm bei der ständig besetzten Stelle des Wachdienstes aus
d) Türöffnungsalarm nach 30 Sekunden
e) Überwachung des Rechenzentrums mittels Bewegungsmeldern
f) Dauer bis Einsatzteam vor Ort: ca. 10 Minuten
g) Meldelinien für Sabotagealarm, Fehlfunktion, usw. vorhanden
h) Wartungsvertrag vorhanden

2. Zugangskontrolle

Maßnahmen zur Verhinderung von unbefugter Systembenutzung.

2.1 Regelung der Zugangsberechtigungen

(bezogen auf Gesamtsysteme oder einzelne Applikationen)

a) Prozesse für die Vergabe und Verwaltung von Zugangsberechtigungen im Mehraugen-Prinzip
b) Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
c) Zugangsberechtigte weisen sich durch personenbezogene Benutzerkennung und Passwort aus
d) Verwaltung der Passwörter von Notfallbenutzern (Administrator, root, usw.)
e) Regelung der Verwendung von Passwörtern durch eine Passwort-Policy
f) Regelung für Sperrung des Arbeitsplatzrechners beim Verlassen
g) Berechtigungen (Kontenaktivierung) für temporäre Mitarbeiter/Externe sind zeitlich befristet
h) Regelung beim Ausscheiden und Wechseln von Berechtigten
i) Regelungen bei Verlust oder Vergessen des Passwortes/Passwörter
j) Begrenzung der Anmeldeversuche
k) Trennen der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen

2.2 Netzwerksicherheit

a) Getrennte Netzwerke für Büro, Services und Gäste
b) Einsatz von Netzwerksicherheitsfunktionen (Network Access Control per 802.1x oder MAC-Filter) die den unbefugten Zugang zum Netzwerk verhindern
c) Schutz des Netzwerks durch die Nutzung von Firewalls und Virenscanner
d) Einsatz von „Intrusion Prevention Systemen“ (IPS) und Absicherung gegen DDOS Angriffe
e) Regelmäßige Kontrolle der Konfigurationen und Abgleich dieser gegen die Vorgaben zur Härtung von Systemen
f) Regelungen zur Freigabe neuer Geräte vor Inbetriebnahme in der produktiven Umgebung

2.3 Zusätzliche Maßnahmen beim Fernzugang

a) Regelung für die Benutzung des Anschlusses, insbesondere bei Benutzung durch Dritte
b) Festlegung der Personen, die zur Anmeldung von außerhalb befugt sind
c) Netzzugangssicherungen durch Hard- und Softwaremaßnahmen – z. B. ausschließlich VPN-Zugänge mit 2-Faktor-Anmeldung
d) Regelungen bei Fernadministration und Fernwartung (Fernwartungskonzept)

e) Regelung für den Fernzugang von Geschäftspartnern (Extranet)
f) Verhinderung des unberechtigten Zugriffs aus dem Internet (Firewall)

2.4 Protokollierung von Zugängen

a) Nachweis der Benutzung von DV-Systemen (Protokollierung der Zugänge)
b) Protokollierung der fehlgeschlagenen Zugangsversuche
c) Protokollierung der Vergabe/Änderung von Zugangsberechtigungen

3. Zugriffskontrolle

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

3.1 Berechtigungskonzept

a) Regelungen für die Vergabe und Verwaltung von Zugriffsberechtigungen
b) Servicebezogene Definition des Berechtigungsmanagement für Eingabe, Kenntnisnahme, Veränderung und Löschung gespeicherter Daten (Detaillierungsgrad, Vergabepraxis, Unterschriftsberechtigung)
c) Individuelle Zugriffsrechte – Bildung von Benutzergruppen
d) Richtlinien für die Dateihaltung (z. B. Verfallsdatum, Aufbewahrungsfristen, Schutzklassen)

3.2 Zugriffsschutz

a) Passwortschutz bei Dateien
b) Trennung von Test- und Produktionsbetrieb
c) Netzzugriffssicherungen
d) Einschränkung der Erlaubnis zur Anwendung von Hilfsprogrammen bzw. Funktionen, die geeignet sind, Sicherheitsmaßnahmen zu umgehen
e) Beschränkung der freien Abfragemöglichkeiten (SQL-Query) von Datenbanken
f) Umsetzung der Löschkonzepte durch automatisierte Löschung von Daten gemäß den jeweiligen Vorhaltezeiten

3.3 Aufbewahrung bei Verwendung von Datenträgern

(Im Folgenden bezogen auf das Rechenzentrum)

a) Regelung, welche Datenträger sich in welchen Zonen befinden dürfen
b) Zonen durch Zutrittskontrollsystem abgesichert
c) Regelung über gesicherte Datenträgeraufbewahrung in Abhängigkeit von der Art der Datenträger (unbeschrieben/neu, beschrieben, etc.)
d) Organisatorische Regelungen zur Datenträgeraufbewahrung (Aufbewahrungsfristen, eindeutige Kennzeichnung von Datenträgern)
e) Festlegung der zur Datenträgerentnahme befugten Personen (Schlüsselverwaltung/-Quittierung, Rückgabe)
f) Keine Reparatur von Datenträgern, sondern grundsätzlich Entsorgung mit Bestätigung der datenrechtlichen Vernichtung und Entsorgungsnachweis
g) Regelung der Anfertigung/Ausgabe von Kopien und Duplikaten (Archivbestände innerhalb und außerhalb des Betriebs, Druckergebnisse, usw.)
h) Regelung der Vernichtung von Datenträgern in Abhängigkeit von der Art der Datenträger (HDD, Magnetbänder, Flashspeicher, Disketten, usw.)

3.4 Protokollierung von Zugriffen

Es gelten die in Ziff. II.2 festgelegten Maßnahmen und zusätzlich folgende:

a) Protokollierung von Lesezugriffen
b) Protokollierung der Vergabe/Änderung von Zugriffsberechtigungen

4. Trennungskontrolle

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

4.1 Mandantentrennung

a) Logische Trennung der Daten
b) Mandantenfähigkeit von Anwendungen
c) Berechtigungskonzept berücksichtigt die Vergabe von Rechten für unterschiedliche Zwecke
d) Trennung von Systemen für Produktion, Test und Entwicklung
e) Restriktiver Einsatz von SQL

4.2 Weitere organisatorische Maßnahmen

a) Innerbetriebliche Vorgaben für die Erhebung und Verarbeitung von Daten
b) Dokumentation der Datenbank(en)
c) Dokumentation der Verarbeitungsprogramme
d) Dokumentation der Datenerhebungszwecke
e) 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 Einsatz von Verschlüsselung

a) Einsatz von Verschlüsselungsroutinen (Datenträger- bzw. Dateiverschlüsselung) gemäß der Risikoklassifizierung
b) Verschlüsselung von Passwörtern
c) Verschlüsselte Übertragung von Daten aus bzw. nach externen Netzen mittels geeigneter Transportprotokolle (SSL/TLS, SSH, S/MIME, PGP, usw.)

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 Regelung der elektronischen Übertragung

a) Verschlüsselte Übertragung von Daten aus bzw. nach externen Netzen mittels geeigneter Transportprotokolle (SSL/TLS, SSH, S/MIME, PGP, usw.)
b) Authentisierung bei Mails (digitale Signatur)
c) Festlegung der Stellen (Dritte), an die durch Einrichtungen der Datenübertragung Daten übermittelt werden können
d) Festlegung der Personen, die zur Übermittlung befugt sind (Berechtigungskonzept)
e) Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege
f) Dokumentation der Abruf- und Übermittlungsprogramme (z. B. FTP = File Transfer Protocol, Firewall, Remote Access)
g) Protokollierung der Datenübermittlung und der Empfänger

1.2 Regelung des Umgangs mit Datenträgern

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

a) Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist nicht vorgesehen
b) Transport von Datenträgern mit personenbezogenen Daten ist nicht vorgesehen

2. Eingabekontrolle

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

2.1 Überwachung und Auswertung

a) Festlegung der Zuständigkeiten für die Dateneingabe (einschließlich Regelung der Stellvertretung)
b) Protokollierung aller Eingaben, Veränderungen oder Löschungen personenbezogener Daten
c) Regelungen für die Umsetzung eines 4-Augen-Prinzips
d) Differenzierte Benutzerrollen (z. B. lesen, schreiben, ändern/löschen)

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 Erstellung und Verwahrung von Sicherheitskopien

a) Generelles Datensicherungskonzept
b) Regelmäßige Sicherung der Benutzerdateien, Datenbanken
c) Namenskonventionen für Sicherungsdateien
d) Kennzeichnung der Datenträger
e) Verwendung des Schreibschutzes bei Datenträgern
f) Bestandsverzeichnis der Sicherungskopien (Dateien, Datenträger)
g) Archivordnung
h) Bestandskontrolle von Datenträgern
i) Protokollierung von Sicherheitsspeicherungen
j) Lagerung von Kopien an besonders geschützten Orten
k) Festlegung von Aufbewahrungsfristen

1.2 Gewährleistung des laufenden Betriebes

a) Stromversorgung:

- Unterbrechungsfreie Stromversorgung durch zwei USV Anlagen für das Rechenzentrum und Notfallarbeitsplätze
- Notstromaggregat mit ausreichendem Treibstoffvorrat
- USV für das NOC mit ausreichender Kapazität (USV Überbrückung bis zu 1 Stunde)
- Regelmäßige Tests der Notstromversorgung (Last- und Leerlauftests)
- Wartungsverträge vorhanden

b) Brandschutz:

- Löschanlage mit Inertgas im Rechenzentrum, Fabrikat Total Walther, Zertifiziert nach VDS, abgenommen nach SprüfV
- Aufschaltung auf die Haus BMZ zur Weiterleitung an die Berufsfeuerwehr
- Zusätzlich Aufschaltung auf die Alarmanlage bei Auslösung (Gasflussmesser im Rohrsystem) mit Weiterleitung auf die ständig besetzte Stelle des Wachdienstes
- Benachrichtigung der verantwortlichen Mitarbeiter der Retarus (Operating, IT-Leitung, Leitung Technik) durch den Wachdienst bei Auslösung
- Optische und akustische Meldung im Rechenzentrum bei Auslösung
- Mehrmals täglich Überprüfung des Tableaus der Retarus-BMZ
- Wartungsvertrag vorhanden

c) Klimatisierung:

- Zwei getrennte Klimatisierungssysteme technisch unterschiedlicher Ausführungen und mit getrennten Leitungswegen
- Neun Innengeräte zur optimalen Kälteverteilung
- Leckage Warnung mit Weiterleitung auf die ständig besetzte Stelle des Wachdienstes
- Benachrichtigung der verantwortlichen Mitarbeiter der Retarus (Operating, IT-Leitung, Leitung Technik) durch den Wachdienst bei Auslösung
- Temperaturüberwachung an mehreren Messpunkten mit Einbindung in das Retarus Operating und Störungsmanagement
- Wartungsvertrag vorhanden

d) IP-Anbindung:

- Redundante Internetanbindung mit getrennter Wegeführung und getrennter Hauseinführung
- Direktzuführungen zum Glasfasercityring des Providers, 24x7x365 Servicevereinbarung

e) Telefonie-Anbindung des Backbones:

- Anbindung an mindestens zwei Carrier
- Permanente Lastverteilung
- 24x7x365 Servicevereinbarung

f) Monitoring:

- 24 x 7 Monitoring von IT-Systemen
- Rufbereitschaften zur Entstörung

g) Redundanzen:

- Hochverfügbarkeit durch den Clusterbetrieb von wichtigen Systemen (Netzwerk, Server, Peripherie)
- Vorhaltung von Ersatz Hardware

1.3 Maßnahmen zum Notfall- und Katastrophenschutz

a) Notfallplan bei Katastrophen (inkl. Zuständigkeiten, Wiederanlaufkonzept, Rufbereitschaften, Ausweichmöglichkeit für Rechenzentrum, usw.)
b) Business-Continuity-Policy (BCM)
c) Disaster-Recovery-Policy (DR)
d) Pandemic Preparedness Plan (PPP)
e) Schutz vor Wassereinbruch
f) Regelmäßige Tests von Bestandteilen der Konzepte

1.4 Organisatorische Maßnahmen

a) Funktionstrennung zwischen Fachabteilung und DV-Abteilung
b) Vertretungsregelungen
c) Zentrale und einheitliche Beschaffung von Hard- und Software
d) Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren
e) Nur Einsatz geprüfter Fremdsoftware
f) Vorgaben für Verfahrens- und Programmdokumentationen
g) Erlass von Dienstanweisungen und Sicherheitsrichtlinien
h) Angemessene Schulung der Anwender
i) Bestellung eines Sicherheitsbeauftragten
j) Wartungsverträge und SLA’s bei Einsatz von Dienstleistern
k) Vorhaltung von Netzwerkplänen

1.5 Weitere technische Maßnahmen

a) Verteilung von IT-Diensten über mehrere Systeme
b) Zentrales *Assetmanagement* von allen eingesetzten Komponenten (CMDB)

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 abgeschlossener 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.

1.3 Aufsichtsbehörden

a) Wenn beim Auftragnehmer eine Prüfung durch die Aufsichtsbehörde stattgefunden hat, so kann der Auftraggeber den Prüfbericht verlangen. Gleiches gilt für Prüfungen bei möglichen Unterauftragnehmern.

2. Management-Systeme

2.1 Datenschutz-Management

a) Bestellter Datenschutzbeauftragter
b) Verpflichtung von Mitarbeitern auf den Datenschutz
c) Betrieb eines Informationssicherheit Management Systems (ISMS)

2.2 Incident-Response-Management

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

2.3 Change-Management

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

2.4 Patch Management

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

2.5 Regelmäßige Überprüfung

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

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