Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO, Stand 01.05.2018

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien (dem creditPass Kunden als Verantwortlicher - nachstehend „**Auftraggeber**“ genannt und der creditPass GmbH als Auftragsverarbeiter - nachstehend „**Auftragnehmer**“ genannt), die sich aus dem zugrundliegenden Vertragsverhältnis betreffend bestimmte IT-Leistungen und weitere elektronische Dienstleistungen ergeben. Hierbei handelt es sich insbesondere nach dem Willen der Parteien und insbesondere des Auftraggebers um den schriftlichen Auftrag zur Auftragsdatenverarbeitung i.S.d. Verordnung (EU) 2016/679 Datenschutz-Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag im Zusammenhang stehen und bei denen Mitarbeiter, Vertreter oder Organe des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers oder eines mit dem Auftraggeber gemäß § 15 f. Aktiengesetz verbundenen Unternehmens in Berührung kommen können. Ergänzend zu den getroffenen Vereinbarungen treffen die Parteien mit dieser Vereinbarung spezielle Regelungen zur Datenverarbeitung im Auftrag.

Diese Vereinbarung zur Auftragsverarbeitung ersetzt vollständig alle vorangegangenen Vereinbarungen dieser Art zwischen den Parteien.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem zugrundliegenden Vertragsverhältnis betreffend bestimmte IT-Leistungen und weitere elektronische Dienstleistungen und den dazugehörigen Anlagen, auf die hier verwiesen wird (nachfolgend „Leistungsvereinbarung“).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung konkret beschrieben.

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 Artt. 44 ff. DSGVO erfüllt sind.

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Mitarbeiterdaten
- ☒ Vertragsabrechnungs- und Zahlungsdaten, einschließlich Bankdaten und Zahlungsabwicklungsdienstleisterdaten
- ☒ Planungs- und Steuerungsdaten
- ☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden (einschließlich Kunden der Kunden)
- Dienstleister
- Mitarbeiter
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und

Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anhang 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(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 unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Soweit diesbezüglich Mehrkosten anfallen, sind diese vom Auftraggeber gegenüber dem Auftragnehmer zu übernehmen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Datenschutzbeauftragte(r) bei dem Auftragnehmer ist:
daspro GmbH
Nikolaus Bertermann, Geschäftsführer
Neues Kranzler Eck
Kurfürstendamm 21
10719 Berlin
T: 030 / 88 77 41 - 50
F: 030 / 88 77 41 - 59
E: bertermann@daspro.de

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich

der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anhang 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Interlake System GmbH	August-Bebel-Str. 26-53 14482 Potsdam	IT Entwicklung und Betrieb
Interlake Media GmbH	August-Bebel-Str. 26-53 14482 Potsdam	IT Entwicklung und Betrieb
Microsoft Ireland Operations Ltd	Dublin 18, Ireland	Microsoft Cloud Deutschland
Colt Technology Services GmbH	Gervinusstr. 18-22 60322 Frankfurt am Main	Netzwerk, Hosting

b) Der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer □bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann 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);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich, spätestens binnen 24h, an den Auftraggeber zu melden;

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich. Hierfür reicht die Textform aus.

(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 Auftraggeber bestätigt oder geändert wird.

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 Aufbewahrungspflichten erforderlich sind.

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

(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.

(4) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

Anhang 1 – Technisch-organisatorische Maßnahmen TOM

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

a) Zutrittskontrolle

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

- Zutritt zu den Rechenzentren nur für autorisierte Mitarbeiter – Prüfung erfolgt durch Sicherheitsdienst und wird protokolliert
- Richtlinie zur Begleitung und Kennzeichnung von Gästen, Ausweiszwang
- Vergabe der Zutrittsberechtigungen zu den Rechenzentren per Richtlinie, nur nach Autorisierung durch den technischen Geschäftsführer
- Server befinden sich in abschließbaren Serverschränken
- Kennzeichnung der Server durch Aliase
- Organisationsanweisung und Protokollierung zur Ausgabe von Schlüsseln und Zugangskarten
- Sicherung durch Wachdienst mit regelmäßigen Kontrollgängen
- Überwachung/Aufzeichnung des Zutritts durch Kameras

b) Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Serversysteme nur mit Passwort und über passwortgeschützte, verschlüsselte Verbindung nutzbar
- Administratorzugriff nur für autorisierte Administratoren über verschlüsselte Verbindungen möglich- Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar
- Remotezugriff nur über verschlüsselte VPN Verbindungen möglich, offene Ports sind durch die Firewalls auf das notwendigste beschränkt
- Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre durch Group Policy
- Verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter
- Verbindliches Verfahren zur Vergabe von Berechtigungen
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern
- Richtlinie zum sicheren, ordnungsgemäßen Umgang und Änderung von Passwörtern sowie der Komplexität von Passwörtern

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, 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:

- Berechtigungsmechanismus mit Möglichkeit zur exakten Differenzierung auf Feldebene
- Verbindliches Berechtigungsvergabeverfahren
- Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Geschäftsführung)
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)
- Einsatz von Application-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen. Verbindliche Arbeitsanweisung für Administratoren im Alarmfall
- Zugriffsauditierung und Analyse der Auditlogs
- Server befinden sich in abschließbaren Serverschränken
- Kennzeichnung der Server durch Aliase

d) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Die Daten unterschiedlicher Auftraggeber/Projekte werden soweit möglich auf unterschiedlichen Systemen verarbeitet
- Einsatz von Virtualisierungstechnologien zur Trennung der Applikation auf logisch unterschiedlichen Systeme
- Einsatz von Sandboxing bei gemeinsam genutzten Applikationssystemen
- Implementierung und Nutzung von Mandantenfähigkeiten
- Die Daten unterschiedlicher Auftraggeber/Projekte werden soweit möglich von unterschiedlichen Mitarbeitern verarbeitet
- Abschottung der Systeme unterschiedlicher Projekte in verschiedenen Sicherheitszonen und physikalische Separierung oder logische Trennung durch Firewalls
- Die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzeptes

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

a) Weitergabekontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Personenbezogene Daten dürfen nur über verschlüsselte Transportwege (Beispiel https, sftp) übertragen werden

- Überprüfung der eingesetzten Verschlüsselung durch Drittanbieter, regelmäßige Anpassung aufgrund von erkannten Sicherheitslücken (bspw. Deaktivierung von als nicht vertrauenswürdigen Ciphern)
- Einsatz von Verschlüsselung in Aufbewahrung und Transport
- Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle
- Automatische Sperre bei mehrmaliger fehlerhafter Authentifizierung
- Einsatz von Application-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen. Verbindliche Arbeitsanweisung für Administratoren im Alarmfall
- Zugriffsauditierung und Analyse der Auditlogs

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des Auftraggebers auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des Dienstleisters
- Applikationsseite Limitierung der Zugriffsarten und der Datentypen pro Rolle und Tätigkeit
- Registrierung von Benutzer und Datum/Uhrzeit von Änderungen
- Einsatz von Application-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen. Verbindliche Arbeitsanweisung für Administratoren im Alarmfall
- Zugriffsauditierung und Analyse der Auditlogs

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backup- und Recovery-Konzept für jedes Serversystem und/oder Applikation mit katastrophensicherer, geschützter Aufbewahrung der Sicherungen (backup vault)
- Nachweis der sicheren und ordnungsgemäßen Archivierung in physisch geschütztem Archiv und verbindlicher Regelung der Zugriffsberechtigten
- Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes
- Einsatz von Storage Systemen mit Redundanz (RAID) wo sinnvoll und notwendig
- Einsatz unterbrechungsfreier Stromversorgung und von Notstromaggregaten
- Richtlinie zur Wartung und Durchführung von Updates
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner)
- Automatisches Monitoringkonzept und permanentes Monitoring zur Erkennung von Störungen sowohl intern als auch extern durch Dienstleister

- Automatisierter Benachrichtigungsworkflow zur Verbreitung von Wartungs- und Störungsmeldungen
- Einsatz von Loadbalancer, Traffic Manager, etc. zur automatisierten Umschaltung auf alternative Systeme

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

a) Datenschutz-Management

- Organisationsanweisung/Richtlinien zu regelmäßigem Training und Datenschutzverpflichtung von Mitarbeitern sowie der internen Organisation zwischen Geschäftsleitung, Datenschutzbeauftragtem und Mitarbeitern
- Ablagesystem für relevante Unterlagen
- Regelmäßige (mindestens einmal jährliche) Überprüfung aller relevanten Unterlagen und Prozesse
- Prozess zur Meldung und Bearbeitung von datenschutzrelevanten Angelegenheiten

b) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- Detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags
- Der Dienstleister hat einen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse