Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO (2016/679)
sowie ggf. zutreffender Landes- oder Kirchen-Datenschutzgesetze
- nachstehend für das jeweils Zutreffende als DSG bezeichnet -

zwischen

_____

_____

_____ _____

- als Verantwortlicher, nachstehend als Auftraggeber bezeichnet -

und der

HiOrg Server GmbH
Dr.-Schier-Str. 9, D-66386 St. Ingbert
vertreten durch den Geschäftsführer Christoph Blechschmitt

- als Auftragsverarbeiter, nachstehend als Auftragnehmer bezeichnet -

- nachstehend einzeln oder gemeinsam auch (Vertrags-) Partei(en) genannt -

Präambel

Die Vertragsparteien haben einen Vertrag über Zusammenarbeit „Nutzung HiOrg-Server“ geschlossen. Auf der Grundlage dieses Vertrages sind sie eine Vereinbarung eingegangen, die ein Auftragsverarbeitungsverhältnis beinhaltet.
Es sind die Regelungen der EU-Verordnung 2016/679 (DSGVO) und des deutschen Bundes-Datenschutzgesetzes (BDSG) zu beachten. Sofern für eine der Vertragsparteien zutreffend, sind auch die Regelungen des Datenschutzgesetzes eines Bundeslandes oder einer Kirche (z.B. DSG-EKD oder KDR-OG) für beide Vertragsparteien zu beachten.
Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der Regelungen des DSG zu konkretisieren, schließen die Parteien die folgende Vereinbarung.
Sie löst einen ggf. vorher zwischen den Vertragsparteien geschlossenen ADV-Vertrag ab.

1. Gegenstand und Dauer des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem ***Nutzungsvertrag HiOrg-Server, § 1 Vertragsgegenstand*** , auf den hier verwiesen wird.
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des ***Nutzungsvertrages HiOrg-Server, § 3 Laufzeit, Kündigungsfristen***.
Unabhängig von den vorstehenden Regelungen zu den Laufzeiten gelten die Verpflichtungen zum Datengeheimnis, die Geheimhaltungspflicht und vereinbarte Aufbewahrungsfristen über das Vertragsende hinaus.

2. Konkretisierung des Auftragsinhalts

Konkretisierung des Zwecks:
Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber dient dem Zweck einer standortunabhängigen Planung, Alarmierung, Durchführung und Abrechnung von Veranstaltungen, Einsätzen oder Lehrgängen, sowie der Verwaltung benötigter materieller und personeller Ressourcen.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des DSG (z.B. Art. 44 ff. DSGVO) erfüllt sind. Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich.

Konkretisierung der Art:
Zur Zweckerfüllung stellt der Auftragnehmer für den Auftraggeber das internetbasierte Datenbanksystem „HiOrg-Server“ mit der erforderlichen Hardware zum Betrieb der zentralen Datenbank und Webapplikation sowie deren Internetanbindung zur Verfügung.

Konkretisierung des Umfangs:
Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber umfasst die Speicherung und Verarbeitung im Datenbanksystem, die Verfügbarkeit über eine Internetanbindung sowie der Sicherung der Datenbestände.

Konkretisierung der Art der Daten:
Gegenstand der Erhebung, Verarbeitung und oder Nutzung personenbezogenen Daten sind folgende Datenarten / -kategorien:

- Name, Vorname, Alias, Passwort, Geburtsdatum und Wohnanschrift,
- Bankverbindung, Beruf, Arbeitgeber, Angehörige, Abwesenheitszeiten,
- Telefonnummern / Fax / E-Mail-Adresse, ggf. weitere Kontaktdaten,
- Foto, Fahrerlaubnis, Kleidergrößen, Ausbildung(en), Prüfungsdaten,
- Mitgliedschaftsdaten, Qualifikation, Dienststellung, Funktion,
- Einsatzzeiten, Einsatzorte, Aufgaben, persönliches Material und Dienstkleidung
- Zeitstempel und IP-Adresse beim Login oder Datenbankänderungen
- Zeitpunkt und Aussagen bei Meldungen, Nachrichten oder Lesebestätigungen
- Ggf. weitere vom Auftragnehmer zusätzlich erfassten personenbezogene Daten (z.B. in dynamisch konfigurierbaren „benutzerdefinierten“ Datenfeldern)
- Lehrberechtigung, Kursteilnahme, BG-Zuordnung (bei Nutzung der Version „HiOrg-Server KURSE“)

Konkretisierung zum Kreis der Betroffenen:
Der Kreis der durch den Umgang ihrer personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Personal / Mitarbeiter des Auftraggebers
- Ansprechpartner, Veranstalter, Kunden, Geschäftspartner des Auftraggebers
- Kursteilnehmer, ggf. deren Arbeitgeber (bei Nutzung der Version „HiOrg-Server KURSE“)

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsfurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe Anlage technische und organisatorische Maßnahmen). Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrages bestehen.
Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Es handelt sich insgesamt 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 zu berücksichtigen.
Auf Grund des technischen Fortschritts, sowie der zu erwartenden Entwicklungen in der Gesetzgebung kann sich eine Notwendigkeit der Anpassung der getroffenen technischen und organisatorischen Maßnahmen ergeben. 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

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.
Unmittelbar durch den Auftragnehmer sicherzustellen sind ein Löschkonzept, das Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers; soweit technisch möglich und datenschutzrechtlich notwendig.
Der Auftragnehmer unterstützt den Auftraggeber auch darüber hinaus nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 DS-GVO.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer ist verpflichtet, im Rahmen der Tätigkeit für den Auftraggeber sämtliche maßgeblichen datenschutzrechtlichen Bestimmungen, sowie die Regelungen dieses Auftrags, einzuhalten. Er verpflichtet sich, beim auftragsgemäßen Umgang mit den personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß DSG zu wahren.
Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.
Zur Wahrung der Vertraulichkeit setzt der Auftragnehmer beim Datenumgang ausschließlich 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.
In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.
Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung aller allgemeinen technischen und organisatorischen Maßnahmen entsprechend DSG zu (siehe Anlage TOM).
Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich 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.
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.
Der Auftragnehmer gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

6. Unterauftragsverhältnisse

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-/Transportleistungen, Wartung und Benutzerservice, Reinigungskräfte 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 Schutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
Der Auftragnehmer ist zur Durchführung dieses Auftrags berechtigt, Unterauftragsverhältnisse mit Rechenzentren zu begründen, über den Betrieb der physikalischen Hardware (Server) und zugehöriger Netzwerkinfrastruktur. Weitere Unterauftragnehmer dürfen nur nach vorheriger ausdrücklicher dokumentierter Zustimmung des Auftraggebers beauftragt werden.
Der Auftragnehmer informiert den Auftraggeber vor Vertragsschluss schriftlich (s. Anlage 1: "Unterauftragsverhältnisse"), welche Unterauftragsverhältnisse er begründet hat, die den Kernbereich (Zweckbestimmung) dieses Auftrags berühren. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).
Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen dieser Vereinbarung 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.
Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gem. DSG, durch Vorlage der Anlage technische und organisatorische Maßnahmen zum Vertrag zur Auftragsverarbeitung, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz).
Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der im DSG (z.B. Art. 32 bis 36 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 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

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

9. Weisungsbefugnis des Auftraggebers

Für die Beurteilung der Zulässigkeit der Erhebung, Verarbeitung oder Nutzung sowie für die Wahrung der Rechte der Betroffenen ist der Auftraggeber verantwortlich. Der Auftraggeber ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die Weisungen bedürfen der Schrift- oder Textform. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
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

Kopien und Duplikate 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.

Nach Abschluss des Auftragsverhältnisses oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten 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. Erfolgt im Rahmen der Kündigung keine besondere Absprache, so wird der Auftragnehmer einen Monat nach Beendigung des Auftragsverhältnisses alle diesem Auftragsverhältnis zugeordneten Datenbestände löschen. Ausgenommen sind Datenbestände, für die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht.
Dokumentationen, die dem Nachweis der 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.

Unterschriften

Ort, Datum	Ort, Datum
Auftraggeber Org.-Kürzel: _____	Auftragnehmer Ch. Blechschmitt Geschäftsführer HiOrg Server GmbH

Hinweis:
Bitte laden Sie die unterzeichnete Vereinbarung direkt in Ihrem HiOrg-Server hoch, im Bereich "System - Mein HiOrg-Server".
Alternativ ist eine Zusendung per E-Mail an **support@hiorg-server.de** oder Fax an **06894-894905-9** möglich.
Eine Rücksendung des Originals per Post ist nicht notwendig!

Anlage 1: Bestehende Unterauftragsverhältnisse

- Ayedo Cloud Solutions GmbH, Halbergstraße 4, 66121 Saarbrücken (Kubernetes)
- cubos Internet GmbH, Goethestraße 5, 52064 Aachen (Prio-SMS)
- Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen (RZ Kernsystem)
- IONOS SE, Elgendorfer Straße 57, 56410 Montabaur (Ticketsystem, DNS, E-Mail)
- LOX24 GmbH, Seestraße 109, 13353 Berlin (SMS)
- netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe (RZ Entwicklung, Webseite, E-Mail)
- rapidmail GmbH, Wentzingerstraße 21, 79106 Freiburg im Breisgau (E-Mail-Versand)
- STRATO AG, Pascalstraße 10, 10587 Berlin (Backupstorage)

Anlage 2: Dokumentation der technischen und organisatorischen Maßnahmen

Dokumentation der technischen und organisatorischen Maßnahmen

- Anlage TOM zur Vereinbarung zur Auftragsverarbeitung -

A. Organisation

Die innerbetriebliche Organisation ist durch folgende Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

- schriftliche Arbeitsanweisungen, Richtlinien, Merkblätter
- Programme/Verfahren sind ordnungsgemäß dokumentiert
- Aufbewahrung/Löschfristen maschinell erzeugter Protokolle/Logs ist geregelt
- Programmfreigabeverfahren ist eingerichtet
- Anwendung des Vier-Augen-Prinzip, z.B. bei physikalischer Datenträgerzerstörung sowie bei weitreichenden Änderungen an Infrastruktur oder Software
- Benachrichtigungen, Auskunftsersuchen, Anliegen bzgl. Berichtigung, Löschung oder Sperrung werden dokumentiert
- Standort sämtlicher von der HiOrg Server GmbH genutzter Server: Deutschland
- keine Nutzung von ausländischen Diensten bei der Verarbeitung von Nutzerdaten

B. Sicherungsmaßnahmen

Unsere Produktiv-Systeme für Applikation, Datenbank, Backup sowie die Georedundanz werden in professionellen deutschen Rechenzentren betrieben und gewartet.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- elektronisches Zutrisstkontrollsystem mit Protokollierung
- Personenkontrolle am Empfang mit Protokollierung
- Richtlinien zur Begleitung und Kennzeichnung von Besuchern
- personalisierte Schlüsselausgabe an Mitarbeiter mit Protokollierung
- Bestreifung des Geländes durch Sicherheitsdienst mit Protokollierung
- Videoüberwachung des Gebäudes im Innen- und Außenbereich
- Einbruchmeldeanlage mit Bewegungs- und Kontaktmeldern
- Im Serverraum sind die Racks und Server nicht näher beschriftet, so dass nicht erkennbar ist, welche Daten welches Unternehmens wo liegen.

1.2. Zugangskontrolle

- Die unbefugte Nutzung der DV-Systeme wird verhindert durch Passwortvergabe und Protokollierung der Passwortnutzung
- Über alle Aktivitäten auf der DV-Anlage werden automatisch Protokolle erstellt
- Die Protokolle werden vom CSO oder der Geschäftsleitung mindestens wöchentlich, sowie bei Auffälligkeiten (z.B. besonders hohe Aktivität) ausgewertet
- Die Datenübertragung von und zum DV-System wird bei kritischen Aktivitäten (z.B. Systempflege, Softwareupdates, Backup) durch folgende Maßnahmen gegen Nutzung durch Unbefugte gesichert: internes Netzwerk (VPN), verschlüsselte Datenübertragung (SSL / HTTPS), Überprüfung bekannter öffentlicher Schlüssel bei Sitzungsbeginn, Protokollierung der Systemnutzung und Protokollauswertung

1.3. Zugriffskontrolle

- Es werden nur die für den jeweiligen Arbeitsplatz relevanten Daten dort vorgehalten. (Entwickler haben z.B. nur Zugriff auf fiktive Testdaten)
- ausschließliche Nutzung festverbauter Datenträger (Festplatten)
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- funktionelle Zuordnung einzelner Datenendgeräte
- automatische Prüfung der Zugriffsberechtigung
- Protokollierung der Systemnutzung und Protokollauswertung
- ausschließliche Menüsteuerung je nach Berechtigung
- differenzierte Zugriffsberechtigung auf Dateien/ Datensätze/ Datenfelder/ Anwendungsprogramme/ Betriebssystem
- differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen)

1.4. Trennungskontrolle

- softwareseitiger Ausschluss (Mandantentrennung)
- Dateiseparierung
- Datenbankprinzip, Trennung über Zugriffsregelung
- Trennung von Test- und Produktionsprogrammen
- Trennung von Test- und Produktionsdaten
- Betrieb mehrerer getrennter Server für jeweils getrennte Aufgabenbereiche (Loadbalancer/Security/SSL, Webserver, Datenbankserver, Backupserver)

1.5. Pseudonymisierung
- Summenbildung und Löschung der Identifikationsmerkmale in den Rohdaten
- Ersetzen von Identifikationsmerkmalen durch Zufallscodes

1.6. Verschlüsselung
- Nutzer-Passwörter werden verschlüsselt in der Datenbank gespeichert
- alle Datenübertragungen erfolgen verschlüsselt (SSL/HTTPS, SSH, TLS)
- Backups werden bei Erstellung auf dem Quell-Gerät verschlüsselt

2. Integrität

2.1. Weitergabekontrolle
- Weitergabe oder Versand von Datenträgern ist generell nicht vorgesehen
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch:
  - Standleitung / internes Netzwerk
  - SSL-Verschlüsselung der Datenübertragung
  - Vollständigkeits- und Richtigkeitsüberprüfung
  - Hardware- und Software-Firewall
  - Intrusion Detection System
  - Virenschutzprogramme

2.2. Eingabekontrolle

Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:
- Protokollierung eingegebener Daten
- Verarbeitungsprotokolle

3. Verfügbarkeit und Belastbarkeit

3.1. Daten werden gegen Zerstörung oder Verlust geschützt durch:
- Einsatz von RAID-Festplattensystemen bei allen Systemen
- mindestens tägliche Sicherung von Daten und Infrastruktur nach Backup-Plan
- Ablage der Backupdaten organisatorisch und geographisch getrennt
- redundante unterbrechungsfreie Stromversorgung
- Einsatz von Netzersatzanlagen
- redundante A/B Stromkreise
- redundante Klimasysteme
- Brandschutzkonzept mit Rauchmeldern
- automatisierte Stickstoff-Löschanlage für Serverräume
- zentrale Überwachungseinheit zur Kontrolle alle Betriebsparameter des Rechenzentrum mit Alarmierung
- Erkennung und Abwehr von DoS-Angriffen durch das Rechenzentrum

3.2. Für alle kritischen Produktivsysteme ist auch softwareseitig eine Hochverfügbarkeitsarchitektur implementiert, mit automatischer Umschaltung und ggf. rascher Wiederherstellbarkeit

3.3. Alle wichtigen Parameter und Dienste der Serversysteme werden von einem engmaschigen automatisierten Monitoring mit Alarmierung überwacht

3.4. Server verfügen über Firewalls und Intrusion-detection-Systeme mit frühzeitiger Sperrung bei Erkennung von wiederholten Zugangs-Fehlversuchen

3.5. Organisationskontrolle:
- Die verarbeiteten Daten werden physikalisch und logisch getrennt von anderen Daten gespeichert
- die Datensicherung erfolgt auf physikalisch, logisch und organisatorisch getrennten Systemen

4. Verfahren zur regelmäßigen Überprüfung und Evaluation
- regelmäßige Überprüfung der Aktualität und -Integrität sämtlicher Backups im Rahmen des automatisierten Monitoring-Systems
- Automatisierte Auswertung aller Server-Logs anhand von Whitelists und manueller Evaluation der verbliebenen Log-Einträge durch den CSO

5. Auftragskontrolle
- schriftliche Vereinbarungen zum Datenschutz zwischen Auftraggeber und Auftragnehmer bzw. Rechenzentrum
- Subunternehmen werden sorgfältig ausgewählt und in derselben Weise vertraglich verpflichtet, wie der Auftragnehmer durch den Auftraggeber verpflichtet ist.
- Mitarbeiter sind zu Verhaltensregeln verpflichtet
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Implementierung unternehmensinterner Datenschutz-Richtlinien
- Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor geplanten Wartungsfenstern oder gravierenden Änderungen
- sämtliche Programmänderungen werden in einem Änderungslog veröffentlicht

Stand der Information: 13.01.2021