Der Vertrag ist bereits digital unterzeichnet und in dieser Form gültig. Bitte drucken Sie diesen aus, unterzeichnen als „Auftraggeber“ und senden uns einen Scan / ein hochauflösendes Foto per E-Mail an datenschutzbeauftragter@jfsb.de zurück.

Alternativ können Sie den Vertrag auch per Post an

Jugend- und Familienstiftung des Landes Berlin
Obentrautstraße 55
10963 Berlin

senden. Erst dann gilt der Vertrag als abgeschlossen.

Bitte füllen Sie die Felder auf Seite 1, 4, 5, und 9 aus.

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen

jugendnetz-berlin.de vertreten durch die

Jugend- und Familienstiftung des Landes Berlin
Obentrautstraße 55
10963 Berlin

– nachfolgend **„Auftragnehmer“** genannt –

und dem Träger

…… ⇦ Trägername

…… ⇦ Einrichtung

…… ⇦ Straße, Hausnummer

…… ⇦ PLZ Ort

– nachfolgend **„Auftraggeber“** genannt –

besteht unter der Kundennummer

K…… ⇦ (Login in der Domainverwaltung)

Ein vom Auftraggeber genutzter Vertrag

1. Gegenstand des Vertrages, Gegenstand dieses Auftragsverarbeitungsvertrages (Art. 28 Abs. 1 DSGVO)

1.1 Gegenstand des Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen bzw. eines (oder mehrerer) dedizierten/dedizierter Webserver(s) sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach vereinbartem Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, FTP-Servers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

1.2 Gegenstand des Vertrages ist **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

1.3 Soweit nachfolgend von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der DSGVO. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung i.S.d. Art. 28 Abs. 1 DSGVO, die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1.4 In **Ergänzung** zu dem/den zwischen den Parteien geschlossenen Vertrag/Verträgen konkretisieren die Vertragsparteien mit vorliegendem Auftragsverarbeitungsvertrag die gegenseitigen Pflichten im generellen Umgang mit den Daten des Auftraggebers.

2. Laufzeit, Beendigung, Löschung von Daten (Art. 28 Abs. 1 DSGVO)

2.1 Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Hosting-Leistungen des Auftragnehmers an den Auftraggeber. Der Auftrag endet, wenn der Auftraggeber keine Hosting-Leistungen des Auftragnehmers, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des Auftragnehmers, mehr in Anspruch nimmt.

2.2 Die Rechte der durch den Datenumgang bei dem Auftragnehmer betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Auftraggeber geltend zu machen. Er, der Auftraggeber, ist allein verantwortlich für die Wahrung dieser Rechte.

2.3 Nach Ende des Auftrags oder auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Daten des Auftraggebers vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Auftraggeber.

2.4 Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an die Auftraggeber weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden

2.5 Der Auftragnehmer hat den Auftraggeber bei der Umsetzung der Rechte der Betroffenen nach Kapitel III der DSGVO, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen der technischen Möglichkeiten, insbesondere hinsichtlich des Charakters der geschuldeten Dienstleistung, zu unterstützen

2.6 Zu einem Datenträgeraustausch gemäß Art. 28 Abs. 3 lit. g DSGVO zwischen den Beteiligten dieser Auftragsverarbeitung kommt es nicht. Insoweit ist eine Rückgabe nicht zu regeln.

3. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten

3.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag.

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

3.2 Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind.

4. Art der Daten und Kreis der Betroffenen (Art. 28 Abs. 3 S. 1 DSGVO)

4.1 Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Auftraggebers gem. Ziff. 1.2 Satz 2 sind folgende Datenarten:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

☐-Personenstammdaten
☐-Kommunikationsdaten (z.B. Telefon, E-Mail)
☐-Veranstaltungsteilnehmer, Besucher
☐-Kunden
☐-Vertragsabrechnungs- und Zahlungsdaten
☐-Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐-Sonstige Daten:

……

4.2 Kreis der Betroffenen

Der Kreis der durch den Umgang mit den Daten gem. Ziff. 1.2 Satz 2 Betroffenen umfasst:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

☐-Kundinnen und Kunden
☐-Interessentinnen und Interessenten
☐-Abonnentinnen und Abonnenten
☐-Beschäftigte
☐-Mitglieder
☐-Teilnehmerinnen und Teilnehmer
☐-Ansprechpartnerinnen und Ansprechpartner
☐-Sonstige Betroffene:

……

5. Pflichten des Auftragnehmers

5.1 Allgemeine Pflichten Art. 28-33 DSGVO

5.1.1 Der Auftragnehmer verpflichtet sich zu einer schriftlichen Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber auf Anforderung, zum Zweck der direkten Kontaktaufnahme, mitgeteilt.

5.1.2 Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, ist dies nur zulässig im Rahmen der vertraglichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer. Soweit der Auftragnehmer Zugriff auf Daten des Auftraggebers hat, verwendet er diese nicht für vertragsfremde Zwecke, insbesondere gibt er diese an Dritte nur weiter, soweit hierzu eine gesetzliche Verpflichtung besteht. Kopien von Daten dürfen nur mit Zustimmung des Auftraggebers erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Verpflichtungen erforderlich sind.

5.1.3 Der Auftragnehmer stellt die Wahrung der Vertraulichkeit entsprechend Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO sicher. Alle Personen, die auftragsgemäß auf die unter Punkt 4.1 aufgeführten Daten des Auftraggebers zugreifen könnten, müssen auf die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung

belehrt werden.

5.1.4 Der Auftragnehmer stellt die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO sicher.

5.1.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei von ihm oder der bei ihm beschäftigten Personen begangenen Verstößen gegen Datenschutzvorschriften. Gleiches gilt im Falle schwerwiegender Störungen des Betriebsablaufs oder anderen Unregelmäßigkeiten im Umgang mit Daten des Auftraggebers. Soweit den Auftraggeber Pflichten nach Art. 32 und 33 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen. Soweit den Auftraggeber Pflichten nach Art. 32-36 DSGVO treffen, z.B. im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten durch Dritte, hat der Auftragnehmer ihn hierbei im Rahmen des Charakters der durch den Auftragnehmer erbrachten Dienstleistung zu unterstützen.

5.2 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

5.2.1 Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft dabei technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust, um den Anforderungen der DSGVO zu entsprechen.

5.2.2 Die Parteien sind sich einig, dass die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Er muss den Auftraggeber hierüber auf Anfrage informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. 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. Wesentliche Änderungen sind zu dokumentieren.

6. Unterauftragsverhältnisse (Art. 28 Abs. 2 u. 4 DSGVO)

6.1 Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen und Benutzerservice, verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt:

- Für Serveradministration und Support
  Steffen Zwanzig, EDV-Service, Harzer Str. 119, 12435 Berlin

- Für Serveradministration und Housing des Servers im Rechenzentrum
  domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning.

6.2 Bei Änderung der vorstehenden Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Auftragnehmern ergeht hierüber eine Information an den Auftraggeber.

6.3 Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem Unterauftragnehmer zu übertragen.

7. Pflichten des Auftraggebers (Art. 24 DSGVO und Art. 13 und 14 DSGVO)

7.1 Der Auftraggeber ist für die Einhaltung der für ihn einschlägigen datenschutzrechtlichen Regelungen verantwortlich.

7.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er Verstöße des Auftragnehmers gegen datenschutzrechtliche Bestimmungen feststellt.

7.3 Den Auftraggeber treffen die sich aus Art. 24 DSGVO und Art. 13 und 14 DSGVO ergebenden Informationspflichten.

8. Weisungsbefugnisse, Berichtigung, Löschung und Sperrung, Rechte Betroffener (Art. 29 i.V.m. 28 DSGVO sowie Kapitel III der DSGVO)

8.1 Der Auftraggeber hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragnehmers insbesondere auch zu Berichtigung, Sperrung,

Löschung etc. nicht bedarf. Soweit eine Mitwirkung des Auftragnehmers erforderlich ist, ist der Auftragnehmer hierzu gegen Erstattung der anfallenden Kosten verpflichtet. Dem Auftraggeber steht in diesem Fall ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung gemäß Art. 29 i.V.m. 28 DSGVO zu. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

8.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten. Ist der Auftraggeber auf Grund geltender Datenschutzgesetze verpflichtet, Auskünfte zur Erhebung, Verarbeitung und / oder Nutzung von Daten zu erteilen, wird der Auftragnehmer den Auftraggeber dabei soweit notwendig bei der Bereitstellung dieser Informationen unterstützen. Eine diesbezügliche Anfrage hat der Auftraggeber schriftlich an den Auftragnehmer zu richten und diesem die hierdurch entstandenen Kosten zu erstatten.

9. Kontrollrechte des Auftraggebers

9.1 Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

9.2. Dem Auftraggeber steht hierzu die durch den Datenschutzbeauftragten des Auftragnehmers erstellte, regelmäßig überarbeitete und den gesetzlichen Anforderungen entsprechende Dokumentation über die vorhandenen technischen und organisatorischen Maßnahmen zur Verfügung.

9.3. Der Auftraggeber hat das Recht, die Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, nach rechtzeitiger vorheriger Anmeldung (3 Wochen) zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung, die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die

entsprechenden Nachweise verfügbar zu machen. Kosten, die dem Auftragnehmer durch seine Unterstützungshandlung entstehen, sind ihm im angemessenen Umfang zu erstatten.

9.4 Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Art. 28 Abs. 1 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass der Auftraggeber sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

9.5 Der Auftragnehmer verpflichtet sich, den Auftraggeber auf Anforderung, die zur Wahrung seiner bei der Verarbeitung der oben genannten Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen. Dies gilt auch, soweit der Auftragnehmer die Kontrolle seiner Unterauftragnehmer für den Auftraggeber durchführt.

10. Salvatorische Klausel, Gerichtsstand

10.1 Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

10.2 Als Gerichtsstand wird Berlin vereinbart.

……, den ……

……
Auftraggeber

……
… Roland Geiger, Auftragnehmer

jfsb
Jugend- und Familienstiftung
des Landes Berlin
Ahrentrautstraße 55 10963 Berlin

<u>Anlage:</u>

Technische und organisatorische Maßnahmen

DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

gem. Anlage zu Art. 32 DSGVO

jugendnetz-berlin.de vertreten durch die

Jugend- und Familienstiftung des Landes Berlin
Obentrautstraße 55
10963 Berlin

1. Präambel

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag definierten IT-Leistungen, welche in den unter Ziffer 2 definierten Rechenzentren erbracht werden.

Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs. 1 d) DSGVO auf ihre Wirksamkeit hin geprüft.

2. Fähigkeit der Vertraulichkeit

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Maßnahmen	
Festgelegte Sicherheitsbereiche	X
Individuelle Zutrittsberechtigungsvergabe	X
Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen	X
Dokumentationen von Zutrittsberechtigungen	X
Zutrittsdokumentation	X
Autorisiertes Wachpersonal - Während der Geschäftszeiten - 24/7 - Sichtkontrollen	X

Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)	X
Besucher-Regulierungen	X
Regelmäßige Kontrollgänge durch das Sicherheitspersonal außerhalb des RZ-Bereiches	X
Automatisches Zuziehen und Verschließen von Türen	X
Schließung aller Gebäudeeingänge, wie Fenster und Türen	X
Zusätzliche mechanische Schutzmaßnahmen für das Erdgeschoss oder die Kellerfenster	X
Büroräume außerhalb der Arbeitszeit sind verschlossen	24/7-Betrieb, daher immer Personal vor Ort
Schutz und Beschränkung der Zutrittswege	X
Transponder- oder schlüsselkartenbasierte Schließanlage	X
Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes	X
Eingezäuntes Gelände inkl. Videoüberwachung	X
Zutrittskontrollsystem mit Chipkarten	X

Zusätzliche Zugangsbeschränkung der Serverräume	X
Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten	X
Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.)	X
Demilitarisierte Zonen	X
Schutz der Infrastruktur durch Einbruchmeldeanlagen	X
Zugangsbeschränkungen für bestimmte IP-Adressbereiche	X
VPN-Beschränkungen	X
Sperrung von nicht erforderlichen Ports	X
Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar)	X
W-LAN-Verschlüsselung	X
Regelmäßige Software-Updates	X
Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich	X
Einschränkung der zeitlichen Gültigkeit der Benutzerkonten	X
Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins	X
Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung	X
Ablauf von Benutzerpasswörtern	X
Erforderliche Mindestkomplexität für Kennwörter	X

Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes	X
Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes	X
Verschlüsselte Speicherung von User-Passwörtern	X
User-Login-Verlauf	X
Vernichtung von physikalischen Medien nach DIN 32757	X
Nutzung eines Aktenvernichters (mindestens Sicherheitsstufe 3 gem. DIN 32757)	X

3. Fähigkeit der Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Maßnahmen
Rollenbasiertes Berechtigungskonzept (Lesen / Schreiben / Ändern / Kopieren / Löschen)
Dokumentation der Vergabe von Zugriffsrechten
Strenge administrative Aufgabentrennung
Protokollierung von externen Support-Prozessen
Dokumentation der Weitergabe von physischen Speichermedien
Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes)
Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff / Berechtigungskonzept

4. Fähigkeit der Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Schutz der Infrastruktur durch Hardware-Firewalls	X
Software-Firewall	X
Antivirus-Software auf allen Systemen	X
Überwachung und Protokollierung von administrativen Systemzugang und von Konfigurationsänderungen	X
Kontrollierter Zugang zu E-Mails und Internet	X
Trennung von Anwendungs- und Administrationszugängen	X
Überwachung und Protokollierung allgemeiner Benutzeraktivität	X
Protokollierung von externen Support-Prozessen	X
Protokollierung von administrativen Änderungen	X
Zugriffsregelungen und Zugriffsverwaltung	X
Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag	X
Unterbrechungsfreie-Stromversorgung (USV)	X
Desaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust	X
Tägliche inkrementelle Datensicherung	X
Wöchentliche vollständige Datensicherung	X
Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen	X

Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich	X
Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern	X
Notfallplan	X
Externe Audits und Sicherheitstests	X
Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer	X

5. Verfahren zur regelmäßigen Überprüfung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Maßnahmen
Regelmäßige Überprüfung der Systemzugangsberechtigungen
Interne- und externe Audits
Disziplinarmaßnahmen im Falle einer Datenschutzverletzung
Regelmäßige Sicherheitsprüfungen
Regelmäßige Kontrolle externer Dienstleister
Regelmäßige Besprechungen mit den bestellten Datenschutzbeauftragten in Bezug auf Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen

6. Schutz vor unrechtmäßigem Zugang zu personenbezogenen Daten

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Maßnahmen
Kontrollierter Zugang zu E-Mails und Internet
Trennung von Anwendungs- und Administrationszugängen
Regelmäßige Sicherheits-Updates
Überwachung und Protokollierung allgemeiner Benutzeraktivität
Verbot der Nutzung von privaten Datenträgern

Rollenabhängige Zugriffsbeschränkungen
Applikationsbasierte Überprüfung der Eingabeberechtigung

7. Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

Maßnahmen
Vertraulichkeitserinnerungen
Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit
Regelmäßige Datenschutz-Unterweisung der Mitarbeiter
Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks
Datentransfer und –Weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
Schriftliche Richtlinien für die Datenübertragung und –Weitergabe
Verbindliche Regeln für die Offenlegung von sensiblen Daten
Datenschutzkonforme Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags
Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
Festgelegte Ansprechpartner für Änderungsanfragen
Kontrollrechte der Auftraggeber bei der Auftragsdatenverarbeitung
Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie der Auftragnehmer selbst

8. Anonymisierung / Pseudonymisierung / Verschlüsselung

Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der vom Auftraggeber zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

9. Belastbarkeit der Systeme

Der Auftragnehmer unternimmt die unter Ziffer 4 dargestellten Maßnahmen um eine Belastbarkeit der IT- Systeme sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der vom Auftragnehmer zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.