

Auftragsverarbeitungsvertrag (v 1.9.0)

zwischen der

Firma

Adresse

PLZ, Ort

nachstehend Auftraggeber genannt

und

punkt.de GmbH
Sophienstraße 187
76185 Karlsruhe

nachstehend Auftragsverarbeiter genannt.

1 Vertragsgegenstand

Der Auftragsverarbeiter verarbeitet im Rahmen von Hosting und Softwaredienstleistungen personenbezogene Daten im Auftrag des Auftraggebers. Zu diesem Zweck wurde zwischen dem Auftraggeber und dem Auftragsverarbeiter ein Dienstleistungsvertrag (Hauptvertrag / Beauftragung / Ticket aus Ticket-System) geschlossen.

Diese Anlage regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung einer Auftragsverarbeitung. Die Vereinbarungen gelten für die Dauer des Leistungsverhältnisses.

Umfang und Dauer der Datenverarbeitung sind im Hauptvertrag festgelegt. Die verarbeiteten Datenarten und der Kreis der Betroffenen sind im Anhang dokumentiert; er ist Bestandteil des vorliegenden Vertrags.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland darf nur erfolgen, wenn die datenschutzrechtlichen Voraussetzungen erfüllt sind (z. B. Angemessenheitsbeschluss der EU-Kommission, Abschluss von Standardvertragsklauseln, Binding Corporate Rules).

2 Verantwortung für die Auftragsverarbeitung

Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich. Der Auftraggeber trägt weiter die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften.

Eine Verwendung der Daten durch den Auftragsverarbeiter für andere als die vertraglich vereinbarten Zwecke ist nicht erlaubt. Der Auftragsverarbeiter ist gegenüber dem Auftraggeber für die Einhaltung der Bestimmungen dieses Vertrags durch seine Mitarbeiter und etwaige Unterauftragnehmer verantwortlich.

3 Rechte und Pflichten des Auftraggebers

Der Auftraggeber ist für die Wahrung und Erfüllung der gesetzlichen Betroffenenrechte zuständig.

Auskunftspflichten

Auskünfte an Betroffene zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person werden ausschließlich vom Auftraggeber beantwortet.

Berichtigung, Sperrung oder Löschung personenbezogener Daten

Die Berichtigung und Löschung von personenbezogenen Daten erfolgt in der Regel durch den Auftraggeber über seinen Systemzugang. Kann der Auftraggeber die Berichtigung, Sperrung oder Löschung aus technischen Gründen nicht selbst vornehmen, weist er den Auftragsverarbeiter an, die erforderlichen Berichtigungen, Sperrungen oder Löschungen vorzunehmen.

Weisungsbefugnis

Der Auftraggeber ist berechtigt, das bestehende Vertragsverhältnis jederzeit durch generelle Weisungen oder Weisungen im Einzelfall (Einzelweisung) zur automatisierten Verarbeitung personenbezogener Daten in schriftlicher Form zu konkretisieren. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich in Form von Jira Tickets bestätigen. Die weisungsberechtigten Personen des Auftraggebers sind im Anhang dokumentiert. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner die Nachfolger bzw. die Vertreter unverzüglich schriftlich mitzuteilen.

Erteilte Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Kontrollbefugnisse

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Dazu ist er berechtigt, nach Anmeldung und zu den üblichen Geschäftszeiten die Datenverarbeitung vor Ort in den Räumlichkeiten des Auftragsverarbeiters zu prüfen und die Vorlage der zur Kontrolle erforderlichen Dokumente zu verlangen.

Die Kontrolle kann von dem betrieblichen Datenschutzbeauftragten oder von sonstigen zuvor benannten Vertretern des Auftraggebers durchgeführt werden.

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

4 Rechte und Pflichten des Auftragsverarbeiters

Weisungsgebundenheit

Der Auftragsverarbeiter erhebt, verarbeitet oder nutzt personenbezogene Daten bei der Erfüllung des Leistungsvertrags ausschließlich im Rahmen der Zweckerfüllung dieses Vertrages und gemäß den Vereinbarungen dieses Vertrags sowie den Weisungen des Auftraggebers, sofern er nicht gesetzlich zu einer anderen Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Weisungsempfänger beim Auftragsverarbeiter sind im Anhang dokumentiert. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner die Nachfolger bzw. die Vertreter unverzüglich schriftlich mitzuteilen.

Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Gegenüber Betroffenen, die sich mit einem Auskunftersuchen an den Auftragsverarbeiter wenden, erfolgt grundsätzlich keine Beauskunftung; sie werden an den Auftraggeber verwiesen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Geheimnisschutz und Datenschutzaufsicht

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Er verpflichtet sich weiter, die ihm vom Auftraggeber zur Verfügung gestellten Unterlagen und Daten sowie die Arbeitsergebnisse nur berechtigten Personen zugänglich zu machen.

Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet. Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Der Auftragsverarbeiter hat einen betrieblichen Datenschutzbeauftragten (DSB) bestellt (Kontakt Daten siehe Anhang).

Der Auftragsverarbeiter stellt dem Auftraggeber die für die Führung des Verfahrensverzeichnis des Auftraggebers erforderlichen Informationen zur Verfügung. Relevante Änderungen des Verfahrens teilt er dem Auftraggeber unverzüglich mit.

Technische und organisatorische Schutzmaßnahmen

Das im Anhang beschriebene Datenschutzkonzept stellt die technischen und organisatorischen Schutzmaßnahmen dar, die passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit nach Stand der Technik und unter Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter ergriffen wurden. Diese Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber das vereinbarte Sicherheitsniveau nicht unterschreiten.

Der Auftragsverarbeiter sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Der Auftragsverarbeiter ist verpflichtet, die vertraglichen Pflichten durch regelmäßige interne Kontrollen zu überprüfen.

Soweit die beim Auftragsverarbeiter getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist nur mit

Zustimmung des Auftraggebers gestattet. Soweit die Daten außerhalb der Firmenräume des Auftragsverarbeiters erfolgen, stellt er durch geeignete Regelungen und Vereinbarungen sicher, dass die Verarbeitung demselben Schutzniveau unterliegt.

Überlassene Datenträger mit personenbezogenen Daten sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragsverarbeiter hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Eine Weitergabe der Daten an Dritte erfolgt nicht. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragsverarbeiter auf Einzelweisung durch den Auftraggeber. In vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe dieser Daten.

Kopien und Duplikate der verarbeiteten personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hier von ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung dienen, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Duldungs- und Mitwirkungspflichten gegenüber dem Auftraggeber

Der Auftragsverarbeiter verpflichtet sich, alle Anfragen von betroffenen Personen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten. Der Auftragsverarbeiter verpflichtet sich weiter, dem Auftraggeber auf Anfrage in Textform alle Auskünfte zu erteilen, die zur Ausübung der gesetzlichen Kontrollpflichten erforderlich sind. Er wird den Auftraggeber bei der Wahrnehmung dieser Kontrollpflichten unterstützen.

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren und zu diesem Zweck die für die Vertragserfüllung relevanten Räumlichkeiten zu den üblichen Geschäftszeiten zu betreten. Der Datenschutzbeauftragte des Auftragsverarbeiters ist nach Möglichkeit hinzuzuziehen.

Bei der Erfüllung der Rechte der betroffenen Personen durch den Auftraggeber sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragsverarbeiter den Auftraggeber soweit möglich angemessen zu unterstützen.

Berichtigung, Sperrung oder Löschung personenbezogener Daten

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnete Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Betroffene, die sich wegen einer Berichtigung oder Löschung eines Datums direkt an den Auftragsverarbeiter wenden, werden an den Auftraggeber verwiesen.

Informationspflicht gegenüber dem Auftraggeber

Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers. Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen datenschutzrechtlichen Pflichten angemessen zu unterstützen.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen.

Beendigung des Vertrages

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Auftraggebers vertragswidrig verweigert.

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten oder vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind nach Beendigung des Vertrags noch für drei volle Kalenderjahre aufzubewahren.

Unterauftragsverhältnisse

Der Auftragsverarbeiter muss dafür Sorge tragen, dass er Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Schutzmaßnahmen sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die gesetzlichen Voraussetzungen dafür erfüllt sind (z. B. Angemessenheitsbeschluss der EU-Kommission, Standardvertragsklauseln, Corporate Binding Rules).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die ihm auferlegten vertraglichen Verpflichtungen erfüllt hat.

Der Auftraggeber erhält auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt, die Dokumentation von Kontrollen und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmer, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

Eine Auflistung der Unterauftragnehmer findet sich im Anhang zu diesem Vertrag.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Erklärt der Auftraggeber innerhalb von vier Wochen nach der Unterrichtung, dass er mit der geplanten Änderung nicht einverstanden ist, steht ihm ein Sonderkündigungsrecht zu.

Auftragskontrolle

Der Auftragsverarbeiter hat die Einhaltung der Pflichten des Subunternehmers zu überprüfen und das Ergebnis der Überprüfung zu dokumentieren; es ist dem Auftraggeber auf Verlangen zugänglich zu machen

5 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder sollte sich im Vertrag eine Lücke finden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der ungültigen Bestimmung oder zur Auffüllung der Lücke soll eine angemessene Regelung treten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Vertragspartner gewollt haben oder nach dem Sinn und Zweck dieses Vertrages gewollt haben würden, wenn sie den Punkt bedacht hätten.

6 Schlussbestimmungen

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung 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.

Es gilt deutsches Recht.

Dieser Vertrag ist in zwei Exemplaren ausgefertigt, wovon eines dem Auftragsverarbeiter ausgehändigt worden ist.

Auftraggeber



Ort, Datum

Unterschrift

punkt.de GmbH (Auftragsverarbeiter):

Karlsruhe, 31.07.2024

Ort, Datum

Unterschrift

7. ANHANG

7.1 Verarbeitete Daten, Betroffene, Weisungsberechtigte und Unterauftragnehmer

Verarbeitete Arten personenbezogener Daten (bitte auswählen und ergänzen):

- Personenstammdaten
- Kommunikationsdaten
- IP Adressen
- Trackingdaten

weitere personenbezogene Daten

Kreis der Betroffenen(bitte auswählen und ergänzen):

- Kunden
- Interessenten
- Beschäftigte
- Ansprechpartner

weitere Betroffene

Weisungsberechtigte Personen des Auftraggebers:

Name	Vorname	E-Mailadresse
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Weisungsempfänger des Auftragsverarbeiters:

- Weisungsempfänger sind alle im Ticketsystem Jira hinterlegten aktiven Mitarbeiter des Auftragnehmers

Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters:

Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Mail: datenschutz@punkt.de

Unterauftragnehmer:

- Hetzner Online GmbH
Industriestraße 25, 91710 Gunzenhausen, Deutschland
- Plus.line AG
Mainzer Landstraße 199, 60326 Frankfurt am Main, Deutschland
- easybill GmbH
Düsselstr. 21, 41564 Kaarst, Deutschland

7.2 Schutzmaßnahmen

Nach Artikel 32 DSGVO vereinbarte technisch-organisatorische Schutzmaßnahmen

Vertraulichkeit:

Sicherungskategorie	Maßnahme
Zutrittskontrolle	<p>Die Systeme des Auftragnehmers werden in einem kommerziellen Rechenzentrum in Frankfurt betrieben. Der Zutritt zum Gebäude ist per Chip & PIN abgesichert. Das gesamte Gebäudeinnere wird mit Kameras überwacht. Das Betreten und Verlassen des Gebäudes wird vom Werksschutz-Personal des RZ-Betreibers überwacht und protokolliert.</p> <p>Innerhalb des Gebäudes stehen dem Auftragnehmer drei verschlossene Racks innerhalb eines mit einem Sicherheitsschloss verriegelten Käfigs zur Verfügung, zu dem außer dem RZ-Betreiber und dem Netzwerk-Dienstleister nur der Auftragnehmer Zutritt hat. Die gesamte Server-Infrastruktur ist Eigentum des Auftragnehmers und wird von diesem eigenverantwortlich betrieben.</p> <p>Die Leistungen des RZ-Betreibers beschränken sich auf Gebäude-Management, Werksschutz, Strom (inkl. Notstrom per Diesel-Aggregat), Kühlung und ggf. Inhouse-Verkabelungen. Der Netzwerk-Dienstleister erbringt die Anbindung an den Internet-Backbone über von ihm verwaltete Switches.</p> <p>Erbringt der Auftragnehmer Entwicklungs- oder Supportleistungen auf Systemen im Verantwortungsbereich des Auftraggebers, so liegen auch die entsprechenden Maßnahmen in der Verantwortung des Auftraggebers.</p> <p>Zusätzlich zu der vom Auftragnehmer selbst betriebenen Hardware nimmt der Auftragnehmer die Leistungen der Fa. Hetzner als Unterauftragnehmer in Anspruch. Dabei kommen exklusiv gemietete („root“) Serversysteme zum Einsatz, die an den Standorten Falkenstein und Helsinki des Unterauftragnehmers betrieben werden. Der Standort Helsinki dient dabei ausschließlich dem Betrieb von Backup-Speichersystemen.</p> <p>Zugriff auf diese Systeme im Betrieb hat einzig der Auftragnehmer. Die weiteren TOMs in diesem Dokument gelten daher ebenso für diese. Physischer Zugriff auf die Server ist dagegen dem Unterauftragnehmer vorbehalten. Dessen techn. Und organisatorische Maßnahmen werden in einem separaten Dokument zur Verfügung gestellt.</p>

Sicherungskategorie	Maßnahme
Zugangs- und Zugriffskontrolle	<p>Es werden ausschließlich Unix/Linux-basierte Server eingesetzt. Der Zugriff auf diese zu administrativen Zwecken erfolgt grundsätzlich über eine verschlüsselte und stark authentifizierte Verbindung (SSH).</p> <p>Hierbei werden individuelle Accounts für jeden Mitarbeiter des Auftragnehmers eingesetzt. Die Logins werden protokolliert.</p> <p>Die Authentifizierung erfolgt dabei ausschließlich über PKI-Verfahren. Passwort-Authentifizierung ist auf allen Systemen global deaktiviert.</p> <p>Bei LAN-Komponenten wie Routern, Switchen und Loadbalancern kommen wo immer möglich verschlüsselte Verbindungen zum Einsatz. Ist dies nicht der Fall, werden private Management-Netze für den Zugriff verwendet.</p> <p>Der Zugriff auf die Systeme durch den Auftragnehmer erfolgt grundsätzlich vom Standort des Auftragnehmers (Karlsruhe) aus. Sollte in Ausnahmefällen ein Bereitschafts-Techniker von einem entfernten Standort zugreifen, geschieht dies über eine VPN-Verbindung zum Netz des Auftragnehmers und ausschließlich vom vertrauenswürdigen Arbeitsplatzrechner (Laptop) des Technikers aus. Ein Zugriff von öffentlichen Arbeitsplätzen oder Systemen Dritter aus erfolgt nicht.</p> <p>Die Zugriffsberechtigungen von Mitarbeitern des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben.</p> <p>Bei Entwicklungs- und Supporttätigkeiten auf Systemen im Verantwortungsbereich des Auftraggebers sollten entsprechend sichere Verfahren zum Einsatz kommen. Die Verantwortung für die Implementierung dieser Verfahren liegt beim Auftraggeber.</p>
Datentrennung	<p>Das System „proServer“ wird in einer virtualisierten Instanz basierend auf FreeBSD „Jail“ Technologie betrieben. Ein Zugriff auf Daten einer Instanz durch Anwendungen einer anderen Instanz ist nach Stand der Technik ausgeschlossen.</p> <p>Bei einem dedizierten System steht eine Maschine dem Auftraggeber exklusiv zur Verfügung. Die Verarbeitung von Daten anderer Kunden auf derselben Maschine findet nicht statt. Nach Vereinbarung kann projektspezifisch ein isoliertes Netz-Segment mit einer dedizierten Firewall zur Verfügung gestellt werden.</p> <p>Der Auftragnehmer empfiehlt dieses Setup (isoliertes Netz und Firewall), sobald personenbezogene Daten der Schutzstufe C und höher nach dem Modell der Landesdatenschutzbeauftragten verarbeitet werden.</p> <p>Im Rahmen der Softwareentwicklung vom Auftragnehmer betriebene „Staging“-Umgebungen haben denselben Aufbau. Entwickler, die eine eigene Instanz der Anwendung auf Ihrem Arbeitsplatzrechner betreiben müssen, verwenden eine getrennte virtuelle Umgebung für jeden Kunden. Die Festplatten der Arbeitsplatzrechner sind verschlüsselt.</p>

Integrität:

Sicherungskategorie	Maßnahme
Auftragskontrolle	<p>Bei Hosting-Diensten werden durch den Auftragnehmer keine Daten aus dem System exportiert.</p> <p>Werden personenbezogene Daten im Rahmen der Softwareentwicklung in nicht anonymisierter Form durch den Auftragnehmer verarbeitet, etwa im Rahmen von Formatkonvertierungen, so erfolgt dies zum einen auf dedizierten „Staging“-Umgebungen, für die dieselben Maßnahmen gelten wie für die Umgebungen im Live-Betrieb. Zum anderen betreiben die Entwicklungs-Mitarbeiter des Auftragnehmers ihre persönlichen Entwicklungsumgebungen ausschließlich auf dedizierten vom Auftragnehmer zur Verfügung gestellten Arbeitsplatzrechnern, deren Festplatten verschlüsselt sind.</p> <p>Alle Mitarbeiter des Auftragnehmers sind mit dem Arbeitsvertrag auf Vertraulichkeit verpflichtet.</p>

Verfügbarkeit:

Sicherungskategorie	Maßnahme
Verfügbarkeitskontrolle	<p>24x7 Überwachung der Verfügbarkeit der zugesicherten Dienste mit Alarmierung der Bereitschaft per SMS.</p> <p>Hochverfügbarkeits-Konfigurationen können in Absprache mit dem Auftraggeber realisiert werden.</p> <p>Es wird eine tägliche Datensicherung durchgeführt. Die Details werden je nach Projekt individuell festgelegt.</p> <p>Alle zentralen Netz-Komponenten sind grundsätzlich redundant ausgelegt. Der Netzwerk-Dienstleister des Auftragnehmers betreibt darüber hinaus mehrere unabhängige Internet-Uplinks zu geeigneten Transit-IP-Anbietern in Deutschland.</p> <p>Gleiches gilt für die Umgebung im Rechenzentrum des Unterauftragnehmers Hetzner.</p>
Datenlöschung	<p>Wird bei Vertragsende individuell geregelt, z.B. durch Übergabe der Festplatten an den Auftraggeber bei dedizierter Hardware oder durch schriftliche Bestätigung des Überschreibens bei einer virtualisierten Umgebung.</p>