Vereinbarung zur Datenverarbeitung im Auftrag („AVV“)

Präambel

Mit dem 25.05.2018 gilt innerhalb der EU die Datenschutzgrundverordnung (DSGVO). Die Verordnung enthält in Art. 28 DSGVO verbindliche Vorgaben, wenn personenbezogene Daten im Auftrag durch andere Stellen verarbeitet werden. Die Auftragsverarbeitung soll nach Art 28 Abs. 3 DSGVO auf Grundlage eines Vertrages erfolgen und die dort festgelegten Inhalte berücksichtigen.

Begrifflichkeiten

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Verarbeitung von personenbezogenen Daten
Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO).

Verantwortlicher
Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Auftragsverarbeiter
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1. Gegenstand und Dauer des Auftrages

(a) Gegenstand

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen sind konkret beschrieben im Hauptvertrag.

(b) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

2. Art(en) der personenbezogenen Daten:

Die Art(en) der personenbezogenen Daten sind im Hauptvertrag beschrieben.

Rechtsgrundlage für die Verarbeitung ist die Erfüllung eines Vertrages. Eine Speicherung der Daten zur Einrichtung Ihres Zugangs kann jederzeit widerrufen werden.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter 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 Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragsverarbeiter 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.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Die konkrete Beschreibung der technischen und organisatorischen Maßnahmen erfolgt in einer separaten **Anlage** zu dieser Vereinbarung.

4. Berichtigung, Einschränkung und Löschung von Daten

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich vorgeschrieben.

Für den Auftragsverarbeiter ist als Beauftragte(r) bestellt:

Gindat GmbH – Gesellschaft für IT-Normierung und Datenschutz

Wetterauer Str. 6
42897 Remscheid

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten

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

(3) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(4) Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

(5) Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

(6) Der Auftragsverarbeiter 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.

6. Unterauftragsverhältnisse

(1) Der Verantwortlich und die verantwortlichen Stellen gestatten dem Auftragsverarbeiter, Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten zu beauftragen. Der Auftragsverarbeiter trägt die Verantwortung für Vertragsverletzungen, die durch seine Unterauftragsverarbeiter zu vertreten sind.

(2) Unterauftragsverarbeiter unterliegen in Bezug auf die Verarbeitung personenbezogener Daten entsprechenden Verpflichtungen, die für den Auftragsverarbeiter als Datenverarbeiter (oder Unterauftragsverarbeiter) gelten.

(3) Vor der Auswahl eines Unterauftragsverarbeiters prüft der Auftragsverarbeiter dessen Maßnahmen zur Wahrung der Sicherheit, des Datenschutzes und der Vertraulichkeit. Unterauftragsverarbeiter können die Anwendung angemessener Sicherheitsmaßnahmen durch Sicherheitszertifikate nachweisen. Andernfalls prüft der Auftragsverarbeiter in regelmäßigen Abständen bei jedem Unterauftragsverarbeiter dessen Sicherheitsmaßnahmen beim Umgang mit Daten.

(4) Der Einsatz von Unterauftragsverarbeitern erfolgt nach Ermessen des Auftragsverarbeiters unter der Voraussetzung, dass folgende Bedingungen eingehalten werden:

   (a) Der Auftragsverarbeiter informiert den Verantwortlichen im Voraus (per E-Mail oder das Support Portal) über jegliche Änderungen der Unterauftragsverarbeiter, die nach dem Wirksamkeitsdatum der Vereinbarung eintreten (mit Ausnahme eines Notfallaustausches oder der ersatzlosen Streichung eines Unterauftragsverarbeiters).

   (b) Der Verantwortliche kann der Beauftragung eines Unterauftragsverarbeiters durch den Auftragsverarbeiter widersprechen, wenn er in Bezug auf die Verarbeitung von personenbezogenen Daten durch den Unterauftragsverarbeiter einen berechtigten Grund für den Widerspruch hat, indem er dies dem Auftragsverarbeiter innerhalb von dreißig (30) Tagen nach Benachrichtigung der Änderung schriftlich mitteilt. Wenn der Verantwortliche der Beauftragung des Unterauftragsverarbeiters widerspricht, werden die Parteien nach Treu und Glauben zusammenkommen, um eine Lösung zu vereinbaren. Der Auftragsverarbeiter kann entscheiden, (i) den Unterauftragsverarbeiter nicht einzusetzen oder (ii) die vom Verantwortlichen in dessen Einspruch geforderten Korrekturmaßnahmen zu ergreifen und den Unterauftragsverarbeiter weiterhin einzusetzen. Wenn keine dieser Optionen auf zumutbare Weise umsetzbar ist und der Verantwortliche seinen Einspruch aus einem

berechtigten Grund aufrechterhält, kann jede Partei die Vereinbarung mit einer Frist von dreißig (30) Tagen nach Erhalt der Mitteilung schriftlich kündigen. Wenn der Verantwortliche nicht innerhalb von dreißig (30) Tagen nach Erhalt der Mitteilung der Änderung Einspruch erhebt, gilt der neue Unterauftragsverarbeiter als vom Verantwortlichen akzeptiert.

(c) Wenn der Einspruch des Verantwortlichen sechzig (60) Tage, nachdem er erhoben wurde, nicht ausgeräumt wurde und der Auftragsverarbeiter keine Kündigungsmitteilung erhalten hat, gilt der Unterauftragsverarbeiter als vom Verantwortlichen akzeptiert.

(5) Der Auftragsverarbeiter kann einen Unterauftragsverarbeiter austauschen, wenn sich der Grund für den Austausch der Kontrolle des Auftragsverarbeiters entzieht. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen so schnell wie möglich über den neuen Unterauftragsverarbeiter. Der Verantwortliche ist berechtigt, gegen einen neuen Unterauftragsverarbeiter Einspruch zu erheben.

7. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Die Gestellung von Mitarbeitern des Auftragsverarbeiters im Rahmen einer solchen Kontrolle ist bis zu einem Umfang von vier Stunden/Jahr kostenlos, ab der fünften Stunde ist der Auftragsverarbeiter berechtigt eine angemessene Vergütung zu verlangen.

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

(3) Der Auftragsverarbeiter kann seinen Pflichten nach den Absätzen 1) und 2) auch erfüllen 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, DIN-ISO 27001).

8. Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen 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 an den Verantwortlichen zu melden
c) die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen. Der Auftragsverarbeitung ist berechtigt für diese Leistung eine angemessene Vergütung zu verlangen.
d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. Weisungsbefugnis des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten des Verantwortlichen ausschließlich entsprechend der Weisung des Verantwortlichen. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

(2) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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 Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Verantwortlichen auf Anforderung zu bestätigen. Entstehen dem Auftragsverarbeiter zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Verantwortliche.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

11. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Schlussbestimmungen

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage zur AVV

IT-Sicherheitskonzept – Technische und organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Der Auftragsverarbeiter erfüllt diesen Anspruch durch folgende(s) Maßnahmen / IT-Sicherheitskonzept:

1. Rechtliche Rahmenbedingungen

Die Einhaltung der jeweils gültigen gesetzlichen Vorschriften oder verbindlichen Vorgaben anderer Institutionen müssen eingehalten werden. Sämtliche dazu erforderlichen Maßnahmen werden an geeigneter Stelle dokumentiert und veröffentlicht. Die im Unternehmen genutzte Software ist nach den rechtlichen Vorgaben zu lizenzieren, die damit verbundene Dokumentation ist aktuell zu halten.

2. Arbeitsplätze

2.1 Verpflichtung / Sensibilisierung

Jeder IT-Benutzer ist der Einhaltung der gesetzlichen Vorgaben und internen Richtlinien verpflichtet. Neben der Kenntnisnahme und Umsetzung entsprechender Informationen gehört dazu auch die Sensibilisierung zur Vermeidung und Erkennung von Störungen, die aus Verletzungen der Vorgaben zur IT-Sicherheit entstehen oder entstehen können.

2.2 Allgemeine Nutzungsregelungen

- die jeweils erlaubte Nutzung ist ausschließlich zu dienstlichen Zwecken gestattet
- nur freigegebene Software darf verwendet werden
- die Nutzung privater Hard- und Software ist nur mit ausdrücklicher Genehmigung zulässig
- Änderungen an Systemeinstellungen, insbesondere Installationen, Deinstallationen oder Konfigurationsänderungen des Basissystems, sind ausschließlich Administratoren erlaubt

2.3 Identity Management

Zur Steuerung und Kontrolle der unterschiedlichsten Berechtigungen und zur Sicherstellung des korrekten Umgangs mit diesen ist eine umfassende Anwenderverwaltung (Identity Management) einzurichten. Darin ist eine vollständige Dokumentation zu mindestens der folgenden Bereiche pro Anwender vorzusehen und aktuell zu halten:

- Assets (Bereitstellung der Hardware, Software-Lizenzen)
- Kritikalität des Arbeitsplatzes (Bezug zu Geschäftsprozess)
- Berechtigungen (Zutritts- und Zugangsberechtigungen)

Des Weiteren sind Prozesse zu definieren, die die Einrichtung und das Ausscheiden von IT-Anwendern regeln.

2.4 Zutritts- und Zugangsregelungen

Der Arbeitsplatz ist aufgeräumt zu halten, so dass Unbefugte keinen Zugriff auf Informationen oder Anwendungen ermöglicht wird. Hierzu finden gesonderte Regelungen Anwendung. Als grundsätzliche Sicherheitsmaßnahme ist zu beachten, dass die Weitergabe von Benutzerkennungen und Passwörtern oder sonstigen Authentifizierungshilfsmitteln untersagt ist. Bei Verdacht, dass die eigene Zugangs- bzw. Zutrittsberechtigung unerlaubt durch Dritte genutzt wurde, sind entsprechende Maßnahmen zu treffen, um die Vertraulichkeit dieser Berechtigungen wiederherzustellen. Es ist eine Übersicht zu erstellen und aktuell zu halten aus der hervorgeht, welche Berechtigungen jeder Anwender hat, insbesondere Zugang zu Daten bzw. Informationen der Klasse „vertraulich“.

2.5 Passwort-Regeln

Es gibt eine interne Passwortrichtlinie. Die Administration ist angehalten, geeignete technische Maßnahmen so einzurichten, dass die Einhaltung für Anwender verständlich und einfach ist und Fehlbedienungen ausgeschlossen sind.

2.6 Sicherheitsupdates

Die Sicherheitseinstellungen sämtlicher IT-Systeme, die der Behebung von Schwachstellen dienen, sind auf aktuellem Stand zu halten („Sicherheitsupdates“).

2.7 Virenschutz

Auf sämtlichen IT-Systemen ist durch die IT ein aktiver und aktueller Virenschutz sicherzustellen. Die eingestellten Konfigurationen dürfen vom Anwender nicht deaktiviert oder verändert werden. Jeder elektronische Datenträger ist vor Verwendung auf Viren oder sonstige Schadprogramme zu untersuchen.

2.8 Verschlüsselung

Der Verschlüsselung kommt eine besondere Bedeutung zu, für die es eine interne Klassifizierungsrichtlinie gibt.

2.9 Notfallvorsorge

Jeder Anwender hat regelmäßige Sicherungen durchzuführen von Dateien, die nicht über zentrale Mechanismen gesichert werden (können). Dabei ist darauf zu achten, dass die Datensicherung verschlüsselt erfolgt, die Datenträger sicher aufbewahrt und in ausreichenden Zeitabständen auf Lesbarkeit überprüft werden.

3. Zentrale Systeme und Netzwerke

3.1 Verfügbarkeit

Abhängig von ihrer Funktion innerhalb von Geschäftsprozessen und den Vereinbarungen mit Nutzern bzw. Nutzergruppen der Systeme ist für diese die geforderte Verfügbarkeit sicherzustellen.

3.2 Monitoring

Es ist ein Monitoring zu etablieren, welches die Kenntnis von Unregelmäßigkeiten des Betriebs in einer angemessenen Zeit ermöglicht. Die Schwerpunkte liegen in der Überwachung der Verfügbarkeit, der sicheren Kommunikation und der Unversehrtheit der Daten. Im Rahmen gesetzlicher Vorschriften ist die sachgerechte Protokollierung und Auswertung relevanter Vorgänge, auch die von Anwenderaktivitäten, einzurichten. Darüber hinaus ist über das Monitoring der Nachweis über die Einhaltung von SLA´s und eine Übersicht über sicherheitsrelevante Vorkommnisse zu erbringen (Reportwesen).

3.3 Zugriffsregelungen

Den Zugriffsregelungen auf das Netz des Auftragsverarbeiters aus öffentlichen Netzen heraus kommt besondere Bedeutung zu. Sie sind entsprechend differenziert erstellt und besonders zu kontrollieren.

3.3.1 Physikalischer Zugang

Der Zugang zu lokalen Netzen, kabelgebunden oder drahtlos, darf nur berechtigten Personen oder Systemen mit eindeutiger Autorisierung möglich sein. Die Bereitstellung von offenen Zugangspunkten ist nur dann erlaubt, wenn gleichzeitig sichergestellt ist, dass keine sicherheitsrelevanten Komponenten berührt werden. Dazu zählen neben physikalischen Systemen und Applikationen insbesondere interne Daten und Informationen.

3.3.2 Authentifizierung

Jeder Nutzer der Infrastruktur des Auftragsverarbeiters hat sich eindeutig zu authentifizieren (personalisierte Anmeldung). Da über die Authentifizierung auch Berechtigungen gesteuert werden sind sog. Gruppen-logins, bei denen sich mehrere Anwender mit derselben Kennung anmelden, nur in besonderen Ausnahmefällen erlaubt. Die damit verbundenen Regelungen (u. a. die interne Passwortrichtlinie) sind zu beachten.

3.3.3 Autorisierung

Ein unbeaufsichtigter bzw. unprotokollierter Zugang zu Daten und Informationen der Klasse „vertraulich“ bzw. „streng vertraulich“ ist zu verhindern. Anfragen zu Zugängen zu Informationen der genannten Klassen sind nur nach Rücksprache mit dem Eigentümer der Information zu bearbeiten.

3.4 Datensicherungskonzept

Sämtliche Daten sind in geeigneter Weise zu sichern. Abhängig ihrer Kritikalität bei Verlust sind der Umfang, die Regelmäßigkeit, die Aufbewahrung, Anforderungen an Wiederherstellbarkeit und mögliche Besonderheiten zu berücksichtigen.

3.5 Change Management

Jede Änderung an der IT-Infrastruktur kann Auswirkungen auf die gesetzten Schutzziele haben und ist nur nach entsprechender Planung und Vorbereitung durchzuführen.

3.6 Desaster Recovery

Die im Rahmen eines „Desaster Recovery“ aufgeführten Maßnahmen betreffen Störfälle, die deutlich über den Umfang zu erwartender Störungen hinausgehen (Katastrophen). Die damit verbundenen besonderen und umfangreichen Maßnahmen können erheblichen Einfluss auf sonstige Organisationen, Prozesse und Richtlinien haben. Das grundlegende Konzept für diese Fälle ist separat erstellt.

4. Externe Sicherheit

Der Bereich der externen Sicherheit umfasst sämtliche Verbindungen von IT-Komponenten zu öffentlichen Umgebungen. Die Schwerpunkte liegen dabei auf den zentralen Übergängen eines internen Netzes in ein öffentliches Netz und den Zugängen einzelner Arbeitsstationen in das interne Netz.

4.1 Zutrittsregelungen

Die im Bereich der Arbeitsplatzsicherheit aufgeführten Anforderungen finden gleichermaßen für den Gebäudeschutz Anwendung. Firmenfremde Personen sind, besonders in sicherheitskritischen Bereichen, ständig zu beaufsichtigen. Je nach Schutzbedarf sind weitere einschränkende Maßnahmen durchzuführen.

4.2 Zugangssteuerung / -Überwachung

Es sind nur Netzübergänge erlaubt, die einen unberechtigten Zugang verhindern und über Protokollierungsmaßnahmen verfügen, die einen derartigen Versuch erkennen lassen. Durch die IT-Administration muss sichergestellt werden, dass nur bekannte und berechtigte Personen Zugang zum

Netzwerk haben. Entsprechende Dokumentationen und Kontrollverfahren sind zu etablieren. Externe Dritte dürfen nur unter Einrichtung solcher Maßnahmen Zugang erhalten, die eine Kontrolle des Zugangs und des Zugriffs erlauben und eine möglicherweise erforderliche sofortige Unterbindung ermöglichen.

4.3 Internet

Dem Übergang ins Internet kommt im Rahmen der Sicherheitsbetrachtungen erhebliche Bedeutung zu. Es muss gewährleistet sein, dass aus dem Internet kein unerkannter unberechtigter Zugriff auf interne IT-Komponenten, besonders der Daten, möglich ist. Bei Erkennen eines unberechtigten Zugriffs sind sofortige Maßnahmen zu dessen Unterbindung zu treffen.