Vereinbarung über Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

dem Verantwortlichen

und

EXEC IT Solutions GmbH
Südstraße 24
56235 Ransbach-Baumbach

(Auftragsverarbeiter)

gemeinsam „die Parteien“

Inhalt

1 Allgemeines 1
2 Gegenstand und Dauer der Auftragsverarbeitung 1
3 Weisungsgebundenheit 1
4 Pflichten des Auftragsverarbeiters 2
5 Pflichten des Verantwortlichen 2
6 Datenschutzbeauftragter 2
7 Zusammenarbeit mit der Aufsichtsbehörde 2
8 Technisch-organisatorische Maßnahmen 3
9 Kontrollrechte 3
10 Subunternehmer 4
11 Haftung 4
12 Vergütung 4
13 Vertragsdauer 5
14 Sonstiges 5

1 Allgemeines

[1] Diese Ergänzungsvereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus den zwischen den Parteien abgeschlossenen jeweiligen Hauptverträgen ergeben.

[2] Sie findet Anwendung auf alle Tätigkeiten, bei denen der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen erhebt, verarbeitet und/oder nutzt. Die nachfolgenden Regelungen sind als Ergänzung zu den Hauptverträgen zu verstehen.

[3] Diese Vereinbarung verwendet dabei die Begrifflichkeiten, die durch den Europäischen Richtlinien- und Verordnungsgeber beim Erlass der Datenschutz-Grundverordnung (DSGVO) verwendet wurden.

[4] Diese Vereinbarung ersetzt alle bisherigen datenschutzrechtlichen Regelungen zwischen den Parteien zur Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen.

2 Gegenstand und Dauer der Auftragsverarbeitung

[1] Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten ausschließlich zur Erfüllung der in den jeweiligen Hauptverträgen näher beschriebenen Leistungen durch den Auftragsverarbeiter für den Verantwortlichen.

[2] Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt.

[3] Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus den vom Verantwortlichen zu führenden Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO. Die Kategorien von Verarbeitungen ergeben sich aus den vom Auftragsverarbeiter zu führenden Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO. Diese finden sich in der Anlage zu dieser Vereinbarung.

[4] Die Dauer der jeweiligen Auftragsverarbeitung entspricht der Laufzeit des jeweiligen Hauptvertrags.

3 Weisungsgebundenheit

[1] Der Auftragsverarbeiter und die ihm unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, verarbeiten die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragsverarbeiter oder der ihm unterstellten natürlichen Person eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragsverarbeiter unterrichtet in derartigen Situationen den Verantwortlichen vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

[2] Mündliche Weisungen bestätigt der Verantwortliche unverzüglich in Textform.

[3] Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere maßgebliche Datenschutzbestimmungen oder sonstige Rechtsgrundlagen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

4 Pflichten des Auftragsverarbeiters

[1] Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben.

[2] Der Auftragsverarbeiter wird den Verantwortlichen mit Rücksicht auf die Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

[3] Der Auftragsverarbeiter wird den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen.

[4] Der Auftragsverarbeiter wird nach Abschluss der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern nicht aufgrund zwingender gesetzlicher Regelungen eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

[5] Der Auftragsverarbeiter führt gemäß Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.

[6] Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er diese dem Verantwortlichen unverzüglich.

5 Pflichten des Verantwortlichen

[1] Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig. Der Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten).

[2] Dem Verantwortlichen obliegen die aus Art. 33, 34 DSGVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

[3] Der Verantwortliche führt gemäß Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.

[4] Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln.

[5] Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten, insbesondere bzgl. datenschutzrechtlicher Bestimmungen, festgestellt werden.

6 Datenschutzbeauftragter

Sofern eine der Parteien zur Benennung eines Datenschutzbeauftragten gemäß Art. 37 DSGVO oder anderer maßgeblicher Rechtsvorschriften verpflichtet ist, teilt sie der jeweils anderen Partei dessen Kontaktdaten sowie jedwede Änderung dieser Daten mit, vgl. Anlage 1.

7 Zusammenarbeit mit der Aufsichtsbehörde

Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgabe zusammen.

8 Technisch-organisatorische Maßnahmen

[1] 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 Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um gemäß Art. 32 DSGVO ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

[2] Zum Nachweis der Erfüllung dieser Maßnahmen kann die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO herangezogen werden.

[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.

[4] Eine Darstellung der jeweiligen vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen ist den Anlagen zu dieser Vereinbarung zu entnehmen.

9 Kontrollrechte

[1] Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der im hiesigen Vertrag niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

[2] Der Verantwortliche hat hierzu das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch einen im Einzelfall zu benennenden, zur Verschwiegenheit verpflichteten, sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen darf, 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 ohne Störung des Betriebsablaufs in dessen Geschäftsbetrieb, soweit aus dringlichen Gründen angezeigt, jedoch nicht häufiger als alle 12 Monate, zu überzeugen.

[3] 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. Der Nachweis solcher Maßnahmen kann durch

a. die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO)

b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren (Art. 42 DSGVO)

c. aktuelle Testate, Berichte, Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer)

d. geeignete Zertifizierung durch IT-Sicherheits-oder Datenschutzaudit (z.B. BSI-Grundschutz)

erfolgen.

[4] Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten, insbesondere bzgl. datenschutzrechtlicher Bestimmungen, feststellt.

10 Subunternehmer

[1] Der Auftragsverarbeiter ist berechtigt, die Dienste weiterer Auftragsverarbeiter nach Maßgabe der jeweiligen Leistungsbeschreibung in Anspruch zu nehmen. Hierbei informiert er den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter. Der Verantwortliche erhält in diesem Fall die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

[2] Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, die im hiesigen Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Hierbei müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des hiesigen Vertrages erfolgt.

11 Haftung

[1] Verantwortlicher und Auftragsverarbeiter haften im Außenverhältnis gegenüber der jeweiligen betroffenen Person für Schäden, die durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wurde, gemeinsam (Art. 82 DSGVO).

[2] Der Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden in Übereinstimmung mit Art. 82 Abs. 2 DSVO nur dann, wenn er

a. seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder

b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder

c. gegen diese Anweisungen gehandelt hat.

[3] Macht ein Betroffener einen Schaden gemäß Absatz 1 gegen den Auftragsverarbeiter geltend, so stellt der Verantwortliche den Auftragsverarbeiter hiervon auf erstes Anfordern frei, sofern der Verantwortliche dem Auftragsverarbeiter im Innenverhältnis nicht eine Verletzung seiner Pflichten gemäß Absatz 2 nachweist.

[4] Im Innenverhältnis gilt darüber hinaus für die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen für Schäden, die aus einem vom Auftragsverarbeiter verursachten Verstoß gegen diese Vereinbarung resultieren:

a. Bei Verstößen aufgrund von Vorsatz oder grober Fahrlässigkeit sowie bei Verstößen gegen das Produkthaftungsgesetz haftet der Auftragsverarbeiter unbegrenzt.

b. Darüber hinaus haftet der Auftragsverarbeiter nur bei Verletzung einer wesentlichen Verpflichtung dieser Vereinbarung und nur in Höhe des bei Vertragsabschluss typischerweise vorhersehbaren Schadens.

[5] Diese Haftungsklausel gilt gleichranging neben anderen, insbesondere in Hauptverträgen, zwischen den Parteien getroffenen Haftungsregelungen.

12 Vergütung

Für Leistungen aus diesem Vertrag, die nicht bereits Leistungsbestandteil des maßgeblichen Hauptvertrags sind und die nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter vom Verantwortlichen eine angemessene Vergütung beanspruchen.

13 Vertragsdauer

[1] Diese Vereinbarung wird auf unbegrenzte Zeit geschlossen. Sie ist von jeder Partei mit einer Frist von 3 Monaten zum Jahresende kündbar.

[2] Durch eine Kündigung dieser Vereinbarung bleiben die Wirksamkeit und Laufzeit von Hauptverträgen unberührt.

[3] Sofern eine Kündigung dieser Vereinbarung durch den Verantwortlichen – ohne Verschulden des Auftragsverarbeiters - dazu führt, dass der Auftragsverarbeiter seiner Leistungspflicht aus einem Hauptvertrag nicht mehr nachkommen kann, ist der Auftragsverarbeiter von der Leistungspflicht hinsichtlich des Umfangs und der Dauer dieser Einschränkung befreit, ohne dass dies den Verantwortlichen von der Zahlung der im Hauptvertrag vereinbarten Vergütung entbindet.

14 Sonstiges

[1] Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang maßgeblichen Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Verantwortlichen liegen.

[2] Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

[3] Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, oder eine an sich notwendige Regelung nicht enthalten sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieses Vertrages nicht berührt.

[4] Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

[5] Gerichtsstand ist Montabaur, sofern das Gesetz nicht zwingend etwas anderes vorschreibt.

(Stand: 01.03.2023)

Datenschutzbeauftragter des Auftragsverarbeiters

(Stand: 01.03.2023)

IT Process & Audit GmbH Wirtschaftsprüfungsgesellschaft
Herr Thomas Martin
Bruder-Kremer-Straße 6
65549 Limburg a. d. Lahn
E-Mail: datenschutzbeauftragter@exec.de
Tel.: +49 (6431) 969-200

Verzeichnis von Verarbeitungstätigkeiten (Auftragsverarbeiter) gemäß Artikel 30 Abs. 2 DSGVO

Bezeichnung der Verarbeitungstätigkeit	Betrieb von Hard- und Software
Auftragsverarbeiter **(Art. 30 Abs. 2 lit. a DSGVO)**	EXEC IT Solutions GmbH Südstraße 24 56235 Ransbach-Baumbach Tel.: 02623 9879 0 E-Mail: info@exec.de
Datenschutzbeauftragter **(Art. 30 Abs. 2 lit. a DSGVO)**	Siehe Vereinbarung zur Auftragsverarbeitung in der jeweils gültigen Fassung.
Verantwortlicher (Auftraggeber) **(Art. 30 Abs. 2 lit. a DSGVO)**	Name und Kontaktdaten s. Einzelvertrag
Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden. **(Art. 30 Abs. 2 lit. b DSGVO)**	Betrieb der im jeweiligen Einzelvertrag aufgeführten Systeme in einem Rechenzentrum. Der Betrieb der Systeme umfasst die Bereitstellung und Überwachung der erforderlichen Fernzugänge, der Server-Hardware und der Systemsoftware.
Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation **(Art. 30 Abs. 2 lit. c DSGVO)**	Eine solche Datenübermittlung findet nicht statt.
Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO **(Art. 30 Abs. 2 lit. d DSGVO)**	s. TOM „Betrieb“
Gültig ab	01.01.2020

Technisch-organisatorische Maßnahmen

Betrieb

Version:	1.4
Stand:	14.12.2022
Nächste Validierung:	01.02.2025

erstellt von:

EXEC IT Solutions GmbH
Südstraße 24
56235 Ransbach-Baumbach
www.exec.de

Inhalt

1 Anwendungsbereich 1

2 Pseudonymisierung 1

3 Verschlüsselung 1

4 Gewährleistung der Vertraulichkeit 1

5 Gewährleistung der Integrität 2

6 Gewährleistung der Verfügbarkeit 3

7 Gewährleistung der Belastbarkeit der Systeme 3

8 Wiederherstellung der Verfügbarkeit 3

9 Regelmäßiger Überprüfung, Bewertung und Evaluierung 4

1 Anwendungsbereich

[1] Dieses Dokument beschreibt die technisch-organisatorischen Maßnahmen gemäß Art. 32 EU-Datenschutzgrundverordnung (DSGVO), die die EXEC IT Solutions GmbH (EXEC) als Auftragsverarbeiter gemäß Art. 30 Abs. 2 lit. d im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DSGVO Abs. 3 lit. c für einen Verantwortlichen ergreift.

[2] Die hier beschriebenen technisch-organisatorischen Maßnahmen gelten für die folgenden Kategorien von durch EXEC als Auftragsverarbeiter im Auftrag eines Verantwortlichen durchgeführte Tätigkeiten:

a. Betrieb von Software in einem von EXEC beauftragten Rechenzentrum

2 Pseudonymisierung

Eine Pseudonymisierung erfolgt ausschließlich auf Weisung des Verantwortlichen im von ihm festgelegten Umfang zu von ihm definierten Zeitpunkten.

3 Verschlüsselung

Maßnahmen zur Verschlüsselung personenbezogener Daten:

a. Jegliche Datenübertragung erfolgt über verschlüsselte Leitungen.

b. Alle mobilen Arbeitsstationen (Notebooks) sind mit verschlüsselten Datenträgern versehen.

c. Die Daten werden auf Backupmedien verschlüsselt gespeichert.

4 Gewährleistung der Vertraulichkeit

[1] Maßnahmen zur räumlichen Zutrittskontrolle, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden:

a. Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe

b. Zutrittskontrollsystem

c. Türsicherungen

d. Werkschutz/ Pförtner

e. Alarmanlage

f. Videoüberwachung

g. Spezielle Schutzvorkehrungen des Serverraums

h. Sperrbereiche

[2] Maßnahmen zur Zugangskontrolle, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird:

a. Persönlicher und individueller User-Login bei Anmeldung am System bzw. Unternehmensnetzwerk

b. Kennwortverfahren

c. BIOS-Passwörter

d. Zusätzlicher System-Login für bestimmte Anwendungen

e. Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität

f. Regelmäßige Softwareaktualisierung / Patching

g. Regelmäßige Schwachstellenscans

[3] Maßnahmen zur Zugriffskontrolle, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

a. Inventarisierung der Informationstechnik

b. Verwaltung und Dokumentation von Berechtigungen

c. Differenzierte Berechtigungen

d. Aufgabenbezogene Profile

e. Aufgabenbezogene Rollen

f. Genehmigungsroutinen

g. Regelmäßige Prüfung der Aktualität von Zugriffsrechten

h. Auswertungen/ Protokollierungen

i. Prüfung/Auditierung

j. Verschlüsselung von externen Datenträgern und Laptops

k. Passwort-Identifikation

l. Logging von Zugriffen auf Systeme

m. Überwachung von Zugriffen auf Systeme

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

a. Verschlüsselung von externen Datenträgern und Laptops

b. Getunnelte Datenfernverbindungen (VPN = Virtual Private Network)

c. Gesichertes WLAN

d. SSL-/TLS-Verschlüsselung

e. Regelungen zur Datenträgervernichtung

5 Gewährleistung der Integrität

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

a. Zugriffsrechte

b. Systemseitige Protokollierungen

c. Funktionelle Verantwortlichkeiten

[2] Maßnahmen zur Auftragskontrolle, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

a. Verbindliche Sicherheitsleitlinien

b. Schulungen aller zugriffsberechtigten Mitarbeiter

c. Regelmäßig stattfindende Nachschulungen

d. Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten

[3] Maßnahmen zur Einhaltung des Trennungsgebots, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können:

a. Getrennte Datenbanken

b. Rechte- und Rollenkonzepte

c. Trennung durch Zugriffsregelungen

6 Gewährleistung der Verfügbarkeit

Maßnahmen zur Verfügbarkeitskontrolle, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können:

a. Service Level Agreements (SLAs) mit Dienstleistern

b. Backup Verfahren

c. Viren-/Schadcodeschutz

d. sichere Aufbewahrung für Backups

e. Redundanz

f. redundante Versorgung

g. Geeignete Archivierungsräumlichkeiten

h. Firewall, IDS/IPS

i. Brandschutz und Löschwasserschutz

j. Monitoring von Alarmen

k. Pläne für Ausfall/ Notfall/ Wiederherstellung

7 Gewährleistung der Belastbarkeit der Systeme

Maßnahmen und Verantwortlichkeiten, um die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen:

a. Automatisiertes Monitoring der Systeme

b. Schwellwerte zur Identifikation von Problemsituationen und Last

c. Regelmäßige Anpassung der Systemressourcen zur Sicherstellung der vereinbarten Leistungen

8 Wiederherstellung der Verfügbarkeit

Maßnahmen und Verantwortlichkeiten, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:

a. Notfallpläne

b. Durchführung von Notfallübungen

9 Regelmäßiger Überprüfung, Bewertung und Evaluierung

Maßnahmen und Verantwortlichkeiten, zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung:

a. Regelmäßige Überprüfung der protokollierten Zugriffe

b. Regelmäßige Bewertung der Maßnahmen durch einen IT-Sicherheitsbeauftragten