

Datenschutzrechtlicher Ergänzungsvertrag

zum Nutzungsvertrag der LizenzID:

zwischen

.....
.....
.....

vertreten durch

– im Folgenden „**Auftraggeber**“ oder **AG**“ genannt –

und

Astaro Services AG, Rheinweg 7, CH-8200 Schaffhausen

– im Folgenden „**Auftragnehmer**“ oder **AN**“ genannt –

Inhaltsverzeichnis

Präambel.....	3
§ 1 Gegenstand und Dauer dieses Vertrages	3
§ 2 Kategorien von Betroffenen und Art der gespeicherten Daten	4
§ 3 Rechte und Pflichten des Auftraggebers	4
§ 4 Allgemeine Pflichten des Auftragnehmers	5
§ 5 Technisch-organisatorische Maßnahmen.....	8
§ 6 Berichtigung, Sperrung und Löschung von Daten	8
§ 7 Löschung von Daten und Rückgabe von Datenträgern.....	8
§ 8 Schadensersatz.....	9
§ 9 Sicherungsrechte	9
§ 10 Allgemeines.....	9
Anlage I:	10
Allgemeine technische und organisatorische Maßnahmen.....	10

Präambel

Der Auftraggeber (AG) hat den Auftragnehmer mit der Archivierung seiner E-Mails beauftragt. Dieser Vertrag wird im folgenden „Grundvertrag“ genannt.

Da es im Rahmen der Installation und Anpassung der vom AN bereitgestellten Speichersysteme sowie in der Folge im Rahmen der Wartung und Pflege jedenfalls nicht ausgeschlossen werden kann, dass der AN Zugriff auf personenbezogene Daten des AG hat, liegt ein Fall der Auftragsdatenverarbeitung vor. Da der Auftraggeber für die Einhaltung des Datenschutzes verantwortlich ist, müssen ergänzend zum Grundvertrag die nachfolgenden Vereinbarungen getroffen werden:

§ 1 Gegenstand und Dauer dieses Vertrages

- 1) Der zwischen Auftragnehmer und dem Auftraggeber geschlossene Grundvertrag umfasst – soweit für diese Vereinbarung von Interesse – die Archivierung von E-Mails. Astaro Mail Archiving („AMA“) bietet die Archivierung von E-Mails als Dienstleistung der Astaro Services AG, Rheinweg 7, CH-8200 Schaffhausen („Astaro“) an. Hierbei werden zu archivierende E-Mails an den zentral über das Internet erreichbaren Archivierungsdienst verschlüsselt übergeben. Die E-Mails werden daraufhin indexiert, archiviert und für autorisierte Benutzer-Anfragen durch den Kunden jederzeit verfügbar gemacht.
- 2) Als cloud-basierte Lösung bietet AMA große Vorteile in Bezug auf Verwaltung, Skalierbarkeit, Verfügbarkeit und Sicherheit. Die Unternehmen der Astaro-Gruppe haben langjährige Erfahrung mit Fragen der Internetsicherheit. Mit dieser umfassenden Expertise hat Astaro einen ganz besonderen Anspruch auf die Sicherstellung des Datenschutzes, Zugriffsschutz und Verfügbarkeit von AMA.
- 3) Dieses Dokument erläutert die internen Abläufe und Strukturen von AMA sowie Schutzmaßnahmen zum umfassenden Daten- und Zugriffsschutz.
- 4) Die AMA-Infrastruktur setzt sich aus einer Vielzahl von Servern zusammen, die unterschiedliche Aufgabenbereiche bearbeiten.
- 5) Astaro unterscheidet hierbei zwischen Production-, Backup- und Control-Cloud welche in jeweils getrennten Hosting-Umgebungen physikalisch und geographisch getrennt arbeiten. Diese Trennung wird auch zu Gewaltenteilung eingesetzt um Zugriffe und Daten maximal zu schützen.

- 6) Der vorliegende Vertrag zur Auftragsdatenverarbeitung hat dieselbe Laufzeit wie der Grundvertrag einschließlich evtl. zugehöriger Folgeverträge und endet somit mit diesem bzw. mit dem letzten Folgevertrag. Davon unberührt bleiben die unter § 4 Abs. 2 vereinbarten Geheimhaltungsverpflichtungen.

§ 2 Kategorien von Betroffenen und Art der gespeicherten Daten

Im Rahmen der unter § 1 aufgeführten Aufgabenbereiche / Leistungen ist ein Zugriff auf personenbezogene Daten möglich. Dies jedoch nur in verschlüsselter Form.

§ 3 Rechte und Pflichten des Auftraggebers

- 1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung / -erhebung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Er bleibt Herr der Daten.
- 2) Der Auftraggeber ist, soweit der Zugriff auf personenbezogene Daten betroffen ist, gegenüber dem Auftragnehmer weisungsbefugt. Der Umgang mit den Daten des AG erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen (in der vorliegenden Vereinbarung sowie im Grundvertrag) und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Vereinbarungen ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er im Einzelfall konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Zuständige Ansprechpartner der Parteien für die Durchführung dieses Vertrages sind dabei:

Auf Seiten des Auftraggebers:

.....
[Name, Kontaktdaten]

Auf Seiten des Auftragnehmers fungiert der unter § 4 Abs. 1 benannte Datenschutzbeauftragte als zentraler Ansprechpartner.

Änderungen sind dem jeweiligen Vertragspartner unverzüglich mitzuteilen.

Ist der Auftragnehmer der Ansicht, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften, so wird er den AG hierauf unverzüglich hinweisen. In einem derartigen Fall ist der Auftragnehmer berechtigt, die Durchführung der entsprechenden Weisung

solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3) Kontrollrechte

Der Auftraggeber hat das Recht, im Einvernehmen mit dem AN die gesetzlich vorgesehene Auftragskontrolle durchzuführen oder durch noch zu benennende Prüfer durchführen zu lassen.

Ebenso hat der AG das Recht, sich vor Beginn der Datenverarbeitung und während der Laufzeit dieser Vereinbarung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der Auftragnehmer wird dem Auftraggeber zu diesem Zweck die Umsetzung der technischen und organisatorischen Maßnahmen, wie in der Anlage beschrieben, nachweisen. Dabei kann dieser Nachweis – soweit nicht nur der konkrete Auftrag betroffen ist – auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Datenschutzauditoren, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

Der AG hat das Recht, sich durch Stichprobenkontrollen, die, soweit dies nicht den Zweck der Kontrolle gefährdet, vorab anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur effektiven Durchführung der Kontrollrechte erforderlichen Auskünfte geben und die entsprechenden Nachweise vorlegen.

§ 4 Allgemeine Pflichten des Auftragnehmers

- 1) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt, der seine Tätigkeit nach den gesetzlichen Vorschriften ausüben kann. Derzeit ist dies:

Herr André Meuser

Tel. +49 (89) 210977-10

e-mail andre.meuser@prw-consulting.de

Der AN wird jeden Wechsel in der Person des Datenschutzbeauftragten dem AG unverzüglich schriftlich mitteilen.

2) Geheimhaltung von Daten

Der Auftragnehmer verpflichtet sich, bei Fernwartungsarbeiten oder Vor-Ort-Maßnahmen auf gespeicherte Daten nur insoweit zuzugreifen, wie es die von ihm zu erbringenden Leistungen erfordern und wie es die nachfolgenden Bestimmungen gestatten.

Der Auftragnehmer wird bei der Verarbeitung und Speicherung von Daten des Auftraggebers technische und organisatorische Maßnahmen so gestalten, dass die Vertraulichkeit der Daten jederzeit gewährleistet ist.

Sollten dem Auftragnehmer Inhalte von Datenbeständen bekannt werden, verpflichtet er sich, diese geheim zu halten.

Der Auftragnehmer wird bei der Vertragserfüllung für den AG diese Verschwiegenheitspflicht und das Datengeheimnis beachten und alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen vertraulich behandeln. Der AN wird alle Mitarbeiter, die mit Daten des AG in Berührung kommen können, schriftlich auf das Datengeheimnis verpflichten und dies dem AG auf Verlangen nachweisen. Der AN wird darauf hinwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, die gesetzlichen Bestimmungen über die Verschwiegenheitspflichten und den Datenschutz beachten und erlangte Informationen nicht an Dritte weitergeben oder in einer sonstigen Art und Weise verwerten und die so begründeten Geheimhaltungspflichten zu überwachen.

Diese Verpflichtungen gelten auch über das Ende des Vertragsverhältnisses hinaus.

3) Unteraufträge

Die Vergabe von Unteraufträgen ist zur Aufgabenerfüllung des Auftragnehmers im Rahmen dieses Vertrages in dem beschriebenen Umfang zulässig. Die Vergabe von weiteren Unteraufträgen ist nur mit vorheriger schriftlicher Genehmigung des Auftraggebers zulässig. Der Auftragnehmer hat den Unterauftragnehmer in gleicher Weise datenschutzrechtlich zu verpflichten, wie er sich gegenüber dem AG verpflichtet hat.

Der AN hat insbesondere auch sicherzustellen, dass der AG die ihm zustehenden Kontrollrechte auch gegenüber dem Unterauftragnehmer ausüben kann.

4) Informationspflichten

Dem Auftragnehmer ist bekannt, dass gesetzliche Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen. Besteht bei dem AN ein Verdacht oder ein konkreter Hinweis, dass personenbezogene Daten des AG an unbefugte Dritte gelangt sind, wird er dies daher schnellstmöglich – ohne Ansehen der Verursachung – dem Auftraggeber melden.

Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat mit dem Auftraggeber einvernehmlich angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für den AG oder für Betroffene zu ergreifen.

5) Sparsame Datenverwendung

Der AN wird jeden Zugriff auf Daten des AG auf das im Rahmen des Grundvertrages unverzichtbare Mindestmaß beschränken. Ist ein Zugriff auf personenbezogene Daten zwingend erforderlich, informiert der Auftragnehmer den Auftraggeber vor dem Zugriff hiervon. Der Auftraggeber entscheidet, wie in derartigen Fällen vorzugehen ist.

Gestattet der Auftraggeber den Zugriff auf ausgewählte personenbezogene Datenbestände, so dürfen die vereinbarten Arbeiten ausschließlich mit diesen Datenbeständen ausgeführt werden.

Soweit wegen der Art der vereinbarten Wartungsarbeiten ein Zugriff auf personenbezogene Daten erfolgt, dürfen keine Veränderungen vorgenommen werden. Versehentlich vorgenommene Veränderungen sind dem Auftraggeber bekannt zu geben.

Änderungen an Systemdateien, die im Zuge der Arbeiten erforderlich geworden sind, müssen vom Auftragnehmer dokumentiert werden. Auf Verlangen des Auftraggebers sind solche Veränderungen nach Abschluss der Arbeiten rückgängig zu machen.

6) Übertragung von Speicherinhalten

Umfasst der Auftrag ein Kopieren gespeicherter Daten, so ist ein Kopierverfahren zu verwenden, das die Anzeige des Inhalts von Datenbeständen so weit wie möglich vermeidet.

Werden während der Wartungsarbeiten zur Fehleranalyse Originaldaten herangezogen, müssen diese nach Beendigung der Maßnahme wieder gelöscht werden.

§ 5 Technisch-organisatorische Maßnahmen

Der Auftragnehmer ist verpflichtet, technisch-organisatorische Maßnahmen zu treffen und während der Dauer des Vertragsverhältnisses aufrechtzuerhalten. Der AN wird diese Maßnahmen dokumentieren.

Soweit anlässlich einer Kontrolle durch den Auftraggeber Anpassungsbedarf festgestellt wird, wird dieser von den Parteien einvernehmlich umgesetzt werden.

Im Einzelnen sind diese Maßnahmen in der **Anlage 1** zu diesem Vertrag festgehalten.

§ 6 Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer darf nur nach Weisung des Auftraggebers Daten, die im Auftrag verarbeitet werden, berichtigen, löschen oder sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und diesen, soweit erforderlich, bei den zu treffenden Maßnahmen unterstützen.

§ 7 Löschung von Daten und Rückgabe von Datenträgern

Jederzeit auf Aufforderung durch den AG, spätestens jedoch mit Beendigung der Vertragslaufzeit, hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem AG unaufgefordert vorzulegen.

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

§ 8 Schadensersatz

Wird der Inhalt von Datenbeständen entgegen der Geheimhaltungspflichten Dritten bekannt, hat der Auftragnehmer dem AG einen hierdurch entstehenden Schaden nach den Regelungen des Grundvertrages zu ersetzen.

Für ein Verschulden seines Personals haftet der Auftragnehmer in gleicher Weise wie für eigenes Verschulden.

§ 9 Sicherungsrechte

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

§ 10 Allgemeines

- 1) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
- 2) Mündliche Nebenabreden zu diesem Vertrag wurden nicht getroffen. Sämtliche Änderungen oder Ergänzungen dieses Vertrages bedürfen der Schriftform. Das gilt auch für die Änderung dieser Schriftformklausel.
- 3) Dieser Vertrag unterliegt deutschem Recht. UN Privatrecht und Kaufvertragsrecht wird ausgeschlossen. Gerichtsstand ist Karlsruhe. Astaro ist jedoch berechtigt, den Kunden auch an dem für dessen Sitz zuständigen Gericht in Anspruch zu nehmen.

....., den

.....
(Auftraggeber)

.....
(Auftragnehmer)

Anlage I:

Allgemeine technische und organisatorische Maßnahmen

Nicht-öffentliche Stellen, 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 EU-Datenschutzvorschriften zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Zur Erfüllung der gesetzlichen Forderungen sind im Gesetz verschiedene Kontrollen definiert, die der Auftragnehmer wie folgt umsetzt:

1) Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden (können), zu verwehren. Der Auftragnehmer muss deshalb dafür Sorge tragen, dass Unbefugte Räume, in denen Daten des Auftraggebers verarbeitet oder gespeichert werden, nicht betreten können und keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (Monitore, Drucker, etc.) erlangen können, auf denen Daten des Auftraggebers verarbeitet oder ausgegeben werden..

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Um das Gebäude des Betreibers zu betreten, ist mittels Transponder und PIN Code die Tür im Eingangsbereich zu öffnen. Hierbei wird jede Person, die sich dort aufhält, durch eine Videokamera erfasst. Die Bilder dieser Kamera werden erfasst und für einen beschränkten Zeitraum gespeichert. Der Zutritt zu einzelnen Serverräumen ist wiederum mittels Transponder und PIN Code nur speziell autorisierten Personen möglich.

Bei Verarbeitung von Daten in externen Datenverarbeitungsanlagen erfolgt die Zutrittskontrolle (bspw. Backup) durch Ausweis-Kontrolle und mehrfach gesicherte Zugangszonen welche mit Kodekarten und PIN gesichert sind.

2) Zugangskontrolle

Unbefugte dürfen keinen Zugang zu den Datenverarbeitungssystemen des Auftragnehmers erlangen können. Daher muss der Auftraggeber die mit der Erfüllung der Leistungen des Grundvertrages beauftragten Personen mit einer sicheren Benutzeridentifikation versehen.

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Der Zugang zu Ressourcen des Rechenzentrums ist durch ein striktes Domänenzugangskonzept gesichert. Die Identifizierung und Authentifizierung an der Domäne erfolgt durch Angabe des Benutzernamens und eines individuellen, komplexen Passwortes welches regelmäßig geändert werden muss. Fehlgeschlagene unberechtigte Zugriffsversuche werden protokolliert und überprüft. Bei Abwesenheit des Benutzers werden die Systeme automatisch gesperrt.

3) Zugriffskontrolle

Es ist zu gewährleisten, dass ausschließlich Personen Zugriff auf die Daten des Auftraggebers erlangen, die mit der Erfüllung des Grundvertrags beschäftigt sind. Dazu sind entsprechende Zugriffsberechtigungsmaßnahmen (Profile, Gruppen, Rollen etc.) einzurichten. Hier sollte ausschließlich nach dem Need-to-Know Prinzip verfahren werden.

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Berechtigungen werden nur nach Freigabe und nur nach dem Need-to-Know Prinzip vergeben. Für die Administration werden soweit technisch möglich, personenbezogene Accounts verwendet. Jedes Benutzerkonto ist dabei jeweils genau einer Person zugeordnet.

Berechtigungen werden nach Rollen bzw. nach, wie von Microsoft empfohlen, in Ressourcen- und Berechtigungsgruppen verschachtelt zugeordnet. Dadurch werden sowohl Berechtigungsänderungen als auch regelmäßige Überprüfungen leichter möglich.

4) Weitergabekontrolle

Der Auftragnehmer muss gewährleisten, dass personenbezogene Daten des Auftraggebers bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Übertragung und Speicherung von personenbezogenen Daten per Email darf nur verschlüsselt erfolgen.

Speicherung, Versand oder Transport von personenbezogenen Daten auf mobilen Datenträgern (DC, USB-Stick, Disk, Speicherkarten etc.) z.B. bei Herausgabe an den Auftraggeber darf nur verschlüsselt erfolgen.

Der Zugriff bei Fernwartungs- bzw. Seviceleistungen auf Daten des Auftraggebers dürfen nur über sichere verschlüsselte Verbindungen erfolgen.

Die jeweiligen sicheren Übertragungswege und Verschlüsselungsverfahren sind regelmäßig an den Stand der Technik gemäß den Empfehlungen des Grundschutzhandbuchs des BSI anzupassen.

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Vom Auftraggeber übergebene Daten werden verschlüsselt transportiert und gespeichert. Hierbei werden die entsprechenden Bereiche auf den Datenträgern durch eine Daten bzw. Festplattenverschlüsselungssoftware verschlüsselt. Es werden dabei nur vom BSI als sicher eingestufte Verschlüsselungsverfahren eingesetzt (z.B. AES256).

5) Eingabekontrolle

Der Auftraggeber muss gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es müssen daher für derartige solche Maßnahmen entsprechende Protokollierungssysteme vorhanden sein.

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Vom Auftragnehmer werden Protokollierungssysteme eingesetzt welche Datenzugriffe, Speicherungen sowie Datensicherungen protokollieren und sichern.

6) Auftragskontrolle

Der Auftragnehmer muss gewährleisten, dass personenbezogenen Daten des Auftragnehmers nur gemäß dessen Weisungen verarbeitet werden. Beschäftigt der Auftragnehmer einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Um eine ordnungsgemäße Bearbeitung von Kundenaufträgen sicherzustellen, sind entsprechende Verarbeitungs- und Änderungsprozesse etabliert worden. Änderungen werden nur in einem kontrollierten Prozess und mit Mitteilung des Auftragnehmers durchgeführt.

7) Verfügbarkeitskontrolle

Der Auftragnehmer muss dafür sorgen, dass personenbezogene Daten des Auftraggebers gegen zufällige Zerstörung oder Verlust geschützt sind. Dazu sind insbesondere folgende Besicherungsmaßnahmen notwendig:

- Einrichtung von entsprechenden Datensicherungsverfahren wie Bandsicherung, Datenspiegelung, Snapshot, etc.
- Räumliche Trennung der Sicherungsdaten.
- Einsatz von unterbrechungsfreien Stromversorgungen, die gewährleistet, dass Daten nicht während der Speicherung oder Übertragung verloren gehen.
- Einrichtung von Schutzmaßnahmen, die Angriffe durch unbefugte Dritte verhindern (Virenschutz, Firewall, Spyware Detection, Paketfilter, DMZ etc.).
- Erstellen von Notfallplänen.

Konkrete Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Um auch möglichst hohe Verfügbarkeit zu gewährleisten werden vom Auftragnehmer eine Vielzahl von Technologien und Prozessen eingesetzt.

Zur Wiederherstellung von Daten im Bedarfsfall werden regelmäßige Datensicherungen in geographisch vom Archivnetzwerk getrennten Speicherzentren durchgeführt. Gespeicherte Daten im Archiv werden immer mittels redundanter Systeme gespeichert.

Um eine unterbrechungsfreie Stromversorgung der Systeme zu gewährleisten sind soweit möglich redundante Netzteile in den Systemen eingebaut. Die Stromzuführung der Systeme ist durch sogenannte USV (Unterbrechungsfreie Stromversorgungen) abgesichert.

Es sind Schutzmaßnahmen eingerichtet um Angriffe durch unbefugte Dritte zu verhindern. Alle Übergänge in unsichere Netzwerke (z.B. Internet) sind durch Firewall Systeme geschützt.

Die jeweiligen Besicherungsmaßnahmen sind regelmäßig an den Stand der Technik gemäß anzupassen.

8) Trennungsgebot

Der Auftraggeber muss dafür sorgen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden.

Die Trennung der Daten muss so gestaltet sein, dass eine „Vermischung“ mit Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers und auch unbefugte Zugriffe Dritter (auch versehentlich) unmöglich sind.

Sollten Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers von behördlichen Zugriffen bzw. Beschlagnahme betroffen sein, muss gewährleistet sein, dass die Daten des Auftraggebers davon unberührt bleiben.

Die Daten des Auftraggebers dürfen nicht zu Testzwecken herangezogen werden.

Maßnahmen des Auftragnehmers zur Umsetzung dieser Verpflichtung:

Um den Netzwerkverkehr unterschiedlicher Auftraggeber voneinander abzuschotten werden sämtliche Daten mit einem dedizierten, dem jeweiligen Auftraggeber zugewiesenen Verschlüsselungszertifikat verschlüsselt. Es ist dabei nicht direkt möglich über den Zugang eines Auftraggebers auf Daten eines anderen Auftraggebers zuzugreifen. Die Verschlüsselungszertifikate werden ferner nur zum Zeitpunkt der Verarbeitung im Hauptspeicher der verarbeitenden Systeme gehalten und sind nicht durch Dritte einsehbar.