Vertrag

über die Verarbeitung personenbezogener Daten im Auftrag

zwischen

der Bundesrechtsanwaltskammer BRAK,
Littenstraße 9, 10179 Berlin

- nachstehend „Auftraggeber" genannt -

und

Atos Information Technology GmbH,

Am Studio 16, 12489 Berlin

- nachstehend „Auftragsverarbeiter" genannt -

Präambel:

Dieser Vertrag über die Verarbeitung personenbezogener Daten im Auftrag tritt als Anhang 1 zur Anlage 10 an die Stelle des bisher bestehenden Vertrags über Auftragsdatenverarbeitung und ist damit Teil des zwischen den Vertragspartnern abgeschlossenen EVB-IT Erstellungsvertrages vom 24.09.2014.

§ 1 Gegenstand der Auftragsverarbeitung

(1) Der Auftraggeber beauftragt den Auftragsverarbeiter wie folgt:

> Realisierung eines Systems zum Betrieb des besonderen elektronischen Anwaltspostfachs sowie dessen Wartung und Pflege

Im Rahmen dieses Auftrages verarbeitet der Auftragsverarbeiter personenbezogene Daten, die er vom Auftraggeber zur Verfügung gestellt bekommt oder im Auftrag des Auftraggebers selbst erhebt.

(2) Die Leistungserbringung erfolgt ausschließlich auf Anforderung und nach Vorgabe des Auftraggebers auf Grundlage des EVB-IT Erstellungsvertrages vom 24.09.2014 einschließlich seiner Anlagen und sämtlicher, z.B. im Rahmen von Änderungsverfahren, getroffenen Zusatzvereinbarungen (nachfolgend als „**Hauptvertrag**“ bezeichnet).

(3) Die Leistungserbringung erfolgt ausschließlich auf Anforderung und nach Weisung des Auftraggebers auf Grundlage des Hauptvertrags.

(4) Gegenstand des Hauptvertrags sind nicht die Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter. Jedoch ist im Zuge der Leistungserbringung des Auftragsverarbeiters als Dienstleister im Bereich der Wartung, des Supports bzw. Administration der Software ein Zugriff auf personenbezogene Daten nicht ausgeschlossen.

(5) Bei der Art der personenbezogenen Daten handelt es sich z.B. um

- Namen
- Kontaktdaten
- Geburtsdaten
- Mitgliedsdaten
- Zugangsdaten der Sicherungsmittel

(6) Der Kreis der Betroffenen umfasst

- Rechtsanwälte und ihre Mitarbeiter
- Vorstände, Geschäftsführung und Mitarbeiter der Rechtsanwaltskammern
- Präsidium, Geschäftsführung und Mitarbeiter des Auftraggebers
- Systemadministratoren
- Richter, Rechtspfleger und Beschäftigte in den Gerichten der Länder und des Bundes
- Richter und Mitarbeiter Anwaltsgerichte
- Mitarbeiter der Landesjustizverwaltungen
- Mitarbeiter in Landes- und Bundesministerien
- Präsidien und Geschäftsführung anderer Berufskammern

§ 2 Pflichten des Auftraggebers

Der Auftraggeber bleibt für die Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung oder -nutzung sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

§ 3 Weisungsrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, in folgendem Umfang Weisungen gegenüber dem Auftragsverarbeiter zu erteilen.

Besteht die Auftragsverarbeitung in der Zurverfügungstellung von Software oder IT-Tools auf Rechnern des Auftragsverarbeiters, erfolgen die Weisungen auch durch Befehlseingaben entsprechend der Funktionalitäten der zur Verfügung gestellten Software oder des IT-Tools.

(2) Der Auftraggeber erteilt alle Weisungen, die zur Erfüllung des Auftrags notwendig sind, in schriftlicher Form. Mündliche Weisungen sind unverzüglich in schriftlicher Form zu bestätigen. Die schriftliche Form wird durch E-Mails oder elektronische Befehlseingaben gewahrt.

(3) Weisungen, die zu einer Änderung oder Ergänzung des Gegenstands der Auftragsverarbeitung führen, sind gemeinsam abzustimmen und entsprechend § 1 dieses Vertrages schriftlich festzuhalten.

(4) Erfolgt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ohne Weisung des Verantwortlichen, weil das Recht der Europäischen Union oder eines Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, ihn zu dieser Verarbeitung verpflichtet, wird der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mitteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(5) Weisungsberechtigte Personen des Auftraggebers sind:

- [redacted]
- [redacted]
- [redacted]

Weisungsempfänger beim Auftragsverarbeiter sind:

- [redacted]
- [redacted]

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner bei Auftraggeber und/oder Auftragsverarbeiter wird dem Vertragspartner unverzüglich ein Nachfolger oder Vertreter schriftlich mitgeteilt.

§ 4 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der datenschutzrechtlichen Pflichten des Auftragsverarbeiters einschließlich der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, die der Auftragsverarbeiter treffen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zu diesem Zweck ist der Auftraggeber insbesondere berechtigt, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, sowie sich durch Stichprobenkontrollen und sonstige Vor-Ort-Kontrollen von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Stichprobenkontrollen und sonstige Vor-Ort-Kontrollen sind in der Regel rechtzeitig beim Auftragsverarbeiter anzumelden. Der Auftraggeber kann von Überprüfungen vor Ort absehen, wenn ihm der Auftragsverarbeiter geeignete Zertifikate, Prüfberichte oder ähnliche Dokumente über die von ihm getroffenen technischen und organisatorischen Maßnahmen zur Verfügung stellt und ihm dadurch die Einhaltung der dort dokumentierten Maßnahmen zum Datenschutz nachweist.

(2) Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder der technischen und organisatorischen Maßnahme feststellt.

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

§ 5 Hauptpflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers zu verarbeiten. Er hat personenbezogene Daten unverzüglich zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in einer Weisung verlangt. Berichtigungen, Löschungen oder Sperrungen von Daten, die im Auftrag verarbeitet werden, erfolgen durch den Auftragsverarbeiter nur nach Weisung des Auftraggebers, es sei denn, der Auftragsverarbeiter ist zur Berichtigung, Löschung oder Sperrung dieser Daten gesetzlich verpflichtet. Verlangt ein Betroffener direkt vom Auftragsverarbeiter die Berichtigung oder Löschung seiner Daten, leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiter.

(2) Dem Auftragsverarbeiter ist es untersagt, die ihm überlassenen Daten für andere Zwecke zu verarbeiten oder ohne Wissen des Auftraggebers Kopien oder Duplikate zu erstellen. 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.

Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber erstellt oder genutzt werden, müssen als Datenträger des Auftraggebers besonders gekennzeichnet und fortlaufend aktualisiert werden. Eingang und Ausgang werden dokumentiert. Die vorstehende Regelung gilt auch für nicht-digitale Datenträger entsprechend.

(3) Der Auftragsverarbeiter ist nicht berechtigt, bei Durchführung seiner vertraglichen Pflichten aus dem Hauptvertrag gezielt auf personenbezogene Daten oder sonstige Betriebsdaten des Auftraggebers zuzugreifen. Sollte ein Zugriff auf personenbezogene Daten des Auftraggebers unerlässlich sein, um die Leistungen aus dem Hauptvertrag erfüllen zu können, beschränkt der Auftragsverarbeiter seinen Zugriff auf das absolut notwendige Maß. Er darf solche personenbezogenen Daten des Auftraggebers nur soweit notwendig auf eigene Rechner übertragen und dort verarbeiten. Die Datenübertragung ist nach dem jeweiligen Stand der Technik zu verschlüsseln. Diese Daten dürfen ausschließlich für den Zweck der Erfüllung der Leistungen aus dem Hauptvertrag verwendet werden. Er ist verpflichtet,

solche Daten nach Durchführung der entsprechenden Leistung aus dem Hauptvertrag unverzüglich zu löschen, spätestens mit Beendigung dieses Vertrages. Dem Auftraggeber steht ein Weisungsrecht zu, wie der Auftragsverarbeiter mit solchen personenbezogenen Daten und sonstigen Betriebsdaten des Auftraggebers zu verfahren hat. Auf Weisung des Auftraggebers sind solche Daten umgehend zu löschen oder auf die Rechner rückzuübertragen. Der Auftragsverarbeiter stellt sicher, dass keine Datenübermittlung an andere Stellen durch den Auftragsverarbeiter erfolgt.

(4) Der Auftragsverarbeiter ist verpflichtet, die Weisungen des Auftraggebers innerhalb seiner Prozesse zu dokumentieren.

(5) Der Auftragsverarbeiter hat ein Löschkonzept vorzuhalten und unmittelbar sicherzustellen, dass die Rechte auf Auskunft und auf Berichtigung sowie, soweit aufgrund datenschutzrechtlicher Bestimmungen vorgeschrieben, auf Vergessenwerden und Datenportabilität erfüllt werden können. Dieser Absatz gilt nur, soweit die betroffenen personenbezogenen Daten auch tatsächlich vom Auftragsverarbeiter auf seinen eigenen Rechnern gespeichert werden.

(6) Der Auftragsverarbeiter hat die datenschutzrechtlichen Grundsätze bei der Verarbeitung personenbezogener Daten einzuhalten sowie die Sicherheit herzustellen, die zum Schutz personenbezogener Datenerforderlich ist. Er ist insbesondere verpflichtet, in seinem Verantwortungsbereich alle technischen und organisatorischen Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen ggf. unter anderem ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten, sofern möglich;

b) die Fähigkeit, die Vertraulichkeit, die Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher zu stellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die

Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden.

Zu diesem Zwecke vereinbaren die Parteien in Anlage 1 zu diesem Vertrag die technischen und organisatorischen Maßnahmen, die erforderlich sind, um ein angemessenes Schutzniveau beim Auftragsverarbeiter sicher zu stellen.

Dem Auftragsverarbeiter ist es gestattet, alternative adäquate technische und organisatorische Maßnahmen aufgrund des technischen Fortschritts und der Weiterentwicklung umzusetzen. Dabei darf das Schutzniveau der in Anlage 1 zu diesem Vertrag vereinbarten technischen und organisatorischen Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind dem Auftraggeber schriftlich mitzuteilen und einvernehmlich in einer geänderten Anlage 1 schriftlich festzuhalten.

(7) Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung alle zur Überprüfung der technischen und organisatorischen Maßnahmen notwendigen Angaben zur Verfügung zu stellen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis von technischen und organisatorischen Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln, mittels derer die Anwendung der datenschutzrechtlichen Bestimmungen präzisiert wird, die datenschutzrechtliche Zertifizierung nach einem genehmigten Zertifizierungsverfahren durch eine akkreditierte Zertifizierungsstelle, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(8) Der Auftragsverarbeiter sichert zu, dass die Daten des Auftraggebers von den sonstigen Datenbeständen des Auftragsverarbeiters strikt getrennt verarbeitet und gespeichert werden. Eine Vermischung der Daten des Auftraggebers mit sonstigen Datenbeständen des Auftragsverarbeiters muss während der gesamten Dauer dieses Vertrages ausgeschlossen sein. Sofern der Auftragsverarbeiter Daten des Auftraggebers für die Ausführung dieses Vertrages nicht mehr benötigt, wird er den Auftraggeber hiervon benachrichtigen und nach Rücksprache mit dem Auftraggeber nicht mehr benötigte Datenbestände löschen. Die Einzelheiten dazu werden die Parteien zu gegebener Zeit festlegen.

§ 6 Mitwirkungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter hat an der Erstellung der Verarbeitungsverzeichnisse des Auftraggebers, die die Auftragsverarbeitung nach § 1 betreffen, mitzuwirken, insbesondere die hierfür erforderlichen Angaben dem Auftraggeber mitzuteilen.

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber des Weiteren bei dessen Einhaltung der Pflichten betreffend die Sicherheit personenbezogener Daten, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehört insbesondere die Unterstützung bei den Pflichten des Auftraggebers,

- ein angemessenes Schutzniveaus durch technische und organisatorische Maßnahmen sicherzustellen, 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, sowie
- Datenschutz-Folgenabschätzungen und
- vorherige Konsultationen mit der Aufsichtsbehörde durchzuführen,

soweit dies jeweils die vertragsgegenständliche Auftragsverarbeitung betrifft.

(3) Der Auftragsverarbeiter sichert zu, dass er bei Datenaudits des Auftraggebers mitwirkt. Werden hierbei Fehler oder Unregelmäßigkeiten festgestellt, wird der Auftraggeber dies dem Auftragsverarbeiter schriftlich mitteilen. Der Auftragsverarbeiter ist verpflichtet, Fehler oder Unregelmäßigkeiten unverzüglich zu beheben.

(4) Der Auftragsverarbeiter ist im Zusammenhang mit der vertragsgegenständlichen Auftragsverarbeitung verpflichtet, den Auftraggeber bei der Beantwortung von Anträgen auf Wahrnehmung von Rechten der betroffenen Personen sowie bei der Einhaltung der Pflichten den Auftraggeber nach den jeweils einschlägigen datenschutzrechtlichen Vorschriften zu unterstützen.

(5) Soweit der Auftraggeber 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. Der Auftragsverarbeiter wird den Auftraggeber insbesondere bei der Erfüllung von dessen Melde- und Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen bei Verletzungen des Schutzes personenbezogener Daten unterstützen sowie dem Auf-

traggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung stellen.

§ 7 Hinweis- und Mitteilungspflichten des Auftragsverarbeiters

(1) Sofern der Auftragsverarbeiter der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Durchführung der entsprechenden Datenverarbeitung solange auszusetzen, bis der Auftraggeber die Weisung bestätigt oder abändert.

(2) Der Auftragsverarbeiter wird den Auftraggeber unverzüglich schriftlich in Kenntnis setzen, sollten im Herrschaftsbereich des Auftragsverarbeiters personenbezogene Daten, die der Auftragsverarbeiter für den Auftraggeber verarbeitet, entgegen den Bestimmungen dieses Vertrages oder der einschlägigen Datenschutzvorschriften verarbeitet werden, verloren gehen oder Dritte auf diese personenbezogenen Daten zugegriffen haben.

(3) Des Weiteren wird der Auftragsverarbeiter den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Auftragsverarbeitung 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.

§ 8 Örtliche Beschränkung der Datenverarbeitung

(1) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union statt. Eine Datenverarbeitung in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum findet nur statt, soweit keine Daten betroffen sind, die Privatgeheimnisse im Sinne von § 203 StGB darstellen, die unter den Beschlagnahmeschutz des § 97 StPO fallen oder die unter die anwaltliche Verschwiegenheitspflicht fallen. Jede darüber hinaus gehende Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn zusätzlich zu den Voraussetzungen des vorstehenden Satzes die besonderen Voraussetzungen der einschlägigen datenschutzrechtlichen Vorschriften, insbesondere die Vorschriften zu Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen, erfüllt sind.

(2) Falls ein Unterauftragsverarbeiter beauftragt werden soll, gelten die vorstehenden Anforderungen auch für den Unterauftragsverarbeiter zusätzlich zu § 9 dieses Vertrages.

§ 9 Unterauftragsverarbeiter

(1) Die Beauftragung von Unterauftragsverarbeitern ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragsverarbeiter Namen und Anschrift des Unterauftragsverarbeiters schriftlich mitteilt. Außerdem muss der Auftragsverarbeiter sicherstellen, dass er den Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Unterauftragsverarbeitern gelten. Insbesondere muss der Auftraggeber berechtigt sein, Kontrollen vor Ort beim Unterauftragsverarbeiter durchzuführen oder durch Dritte durchführen zu lassen. Zudem hat der Auftragsverarbeiter die Einhaltung der Pflichten durch den Unterauftragsverarbeiter regelmäßig zu überprüfen und das Ergebnis dieser Überprüfungen dem Auftraggeber mitzuteilen, soweit dies für die hierin vereinbarte Auftragsverarbeitung relevant ist.

(2) Die Weiterleitung von Daten des Auftraggebers durch den Auftragsverarbeiter an einen Unterauftragsverarbeiter ist erst zulässig, wenn diesem in einem Vertrag dieselben Datenschutzpflichten auferlegt werden, die in diesem Vertrag zwischen dem Auftraggeber und dem Auftragsverarbeiter festlegt sind, wobei insbesondere hinreichende Nachweise dafür erbracht werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen beim Unterauftragsverarbeiter so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der anwendbaren datenschutzrechtlichen Vorschriften erfolgt. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten die sich beim Unterauftragsnehmer bei der Verarbeitung von Daten des Auftraggebers ereignen.

(4) Der Auftragsverarbeiter ist auch ohne schriftliche Zustimmung des Auftraggebers berechtigt, Dritte mit Nebenleistungen, die nicht direkt mit der beauftragten Datenverarbeitung in Zusammenhang stehen, zur Unterstützung bei der Auftragsdurchführung in Anspruch zu nehmen (wie z.B. Telekommunikationsleistungen, Wartung, Pflege und Benutzerservice der eingesetzten Software, Reinigungsdienste, Prüfungs- und Entsorgungsleistungen bezüglich der verwendeten Daten und Datenträger). Der Auftragsverarbeiter ist allerdings verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch mit

diesen Dritten eine schriftliche Vereinbarung zu treffen, die den gesetzlichen datenschutzrechtlichen Vorgaben und Pflichten des Auftragsverarbeiters entsprechen. Der Auftragsverarbeiter gewährt dem Auftraggeber bei Bedarf zu Kontrollzwecken Einsicht unter Berücksichtigung etwaiger vertraglicher Vertraulichkeitsvereinbarungen in die entsprechenden Vertragspassagen.

§ 10 Rückgabe oder Löschung von Daten und Datenträgern

(1) Nach Abschluss des Auftrags oder früher nach Aufforderung durch den Auftraggeber wird der Auftragsverarbeiter alle personenbezogenen Daten und sämtliche in seinen Besitz gelangten Datenträger, Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers entweder an diesen zurückgeben oder datenschutzgerecht löschen oder vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll einer Löschung ist dem Auftraggeber auf dessen Anforderung hin vorzulegen.

(2) Etwaige gesetzliche Aufbewahrungsfristen bleiben hiervon unberührt. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 11 Besondere Vertraulichkeitsvereinbarung; Pflicht zur Wahrung des Datengeheimnisses

(1) Der Auftragsverarbeiter sichert die Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten zu. Er verpflichtet sich, sicherzustellen, dass die ihm unterstellen Personen, die Zugang zu personenbezogenen Daten des Auftraggebers haben, diese Daten ausschließlich auf Weisung des Auftraggebers verarbeiten. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben sowie das Datengeheimnis und, soweit einschlägig, das Fernmeldegeheimnis wahren. Der Auftragsverarbeiter darf ausschließlich Personen einsetzen, die sich ihm gegenüber schriftlich zur Vertraulichkeit verpflichtet haben. Die Verschwiegenheitspflicht erstreckt sich auch auf die dem Auftragsverarbeiter bekannt gewordenen sonstigen Betriebs- und Geschäftsdaten des Auftraggebers. Diese Verschwiegenheitspflicht setzt nicht voraus, dass Daten als vertraulich gekennzeichnet sind. Schaltet der Auftragsverarbeiter Unterauftragsverarbeiter ein, muss er zudem sicherstellen, dass auch diese Unterauftragsverarbeiter und die ihnen unterstellten Personen personenbezogene Daten ausschließlich auf Weisung des Auftraggebers verarbeiten und sich zur Vertraulichkeit im vorstehend vereinbarten Umfang verpflichtet haben.

(2) Der Auftragsverarbeiter verwendet die Daten, überlassene Datenträger und Unterlagen sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen nicht für andere als die gemäß diesem Auftrag definierten Zwecke und verwahrt diese in einer Weise, dass sie Dritten nicht zugänglich sind und gibt diese nicht an Dritte weiter. Auf Verlangen des Auftraggebers hat der Auftragsverarbeiter unverzüglich sämtliche in seiner Verfügungsmacht befindlichen Datenträger des Auftraggebers sowie jegliche Kopien oder Reproduktionen hiervon an den Auftraggeber zurückzugeben oder datenschutzgerecht zu vernichten und dies dem Auftraggeber schriftlich zu bestätigen.

(3) Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial, sofern dieses anfällt, übernimmt der Auftragsverarbeiter standardmäßig. In besonderen vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(4) Vorbehaltlich zwingender gesetzlicher Regelungen verpflichtet sich der Auftragsverarbeiter, weder das Vorhandensein noch den Inhalt bestimmter Daten Dritten zu offenbaren.

(5) Soweit keine anderweitigen gesetzlichen oder vertraglichen Verpflichtungen zur Vertraulichkeit bestehen, entfällt die Vertraulichkeitsverpflichtung gemäß den vorstehenden Bestimmungen, soweit:

- Daten öffentlich bekannt sind oder werden, ohne dass dies auf eine rechts- oder vertragswidrige Handlung des Auftragsverarbeiters zurückzuführen ist oder
- der Auftraggeber Daten gegenüber dem Auftragsverarbeiter schriftlich zur anderweitigen Nutzung freigegeben hat.

(6) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.

Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Auftragsverarbeitung beschäftigten Mitarbeiter und jede sonstige dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Der Auftragsverarbeiter überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften.

(7) Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 12 Eigentums- und Nutzungsrechte

(1) Durch diesen Vertrag werden dem Auftragsverarbeiter keine Nutzungsrechte an den Daten des Auftraggebers gewährt, die über die vertragsgemäße Erfüllung der Auftragsverarbeitung hinausgehen.

(2) Die Daten des Auftraggebers sowie alle von ihm übergebenen Datenträger bleiben im Eigentum des Auftraggebers. Dem Auftragsverarbeiter stehen daran keine Zurückbehaltungsrechte zu.

§ 13 Haftung

(1) Der Auftragsverarbeiter trägt die Darlegungs- und Beweislast dafür, dass er vor Beginn sowie während der gesamten Dauer der Auftragsverarbeitung für den Auftraggeber die Umsetzung der technischen und organisatorischen Maßnahmen, wie in Anlage 1 dieses Vertrages vereinbart, sowie die Einhaltung aller sonstigen ihm in seiner Eigenschaft als Auftragsverarbeiter obliegenden datenschutzrechtlichen Pflichten sichergestellt hat.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen eines Verstoßes gegen datenschutzrechtliche Vorschriften oder, soweit einschlägig, gegen das Fernmeldegeheimnis als auch wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverarbeitungsverhältnisses erleidet, ist im Verhältnis zum Auftraggeber der Auftragsverarbeiter verantwortlich, es sei denn, der Auftragsverarbeiter hat die unzulässige oder unrichtige Datenverarbeitung nicht zu vertreten. Dem Auftraggeber stehen insoweit vertragliche Regressansprüche gegen den Auftragsverarbeiter zu, sollte der Auftraggeber den Betroffenen dieser Schäden entschädigen müssen.

(3) Im Falle einer Verletzung seiner Pflichten aus diesem Vertrag haftet der Auftragsverarbeiter entsprechend den gesetzlichen Regelungen nach Art. 82 DSGVO.

§ 14 Beginn und Dauer des Vertrags; Kündigung

(1) Dieser Vertrag beginnt mit Unterzeichnung durch beide Parteien und gilt für die Dauer des EVB-IT Erstellungsvertrages vom 24.09.2014, ohne dass jedoch für den Auftraggeber eine tatsächliche Verpflichtung zur regelmäßigen Abnahme von Leistungen entsteht.

(2) Das Recht jeder Partei zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Der Auftraggeber kann insbesondere den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen diese Vereinbarung vorliegt, wenn der Auftragsverarbeiter eine

Weisung nicht ausführt oder wenn der Auftragsverarbeiter Kontrollen durch den Auftraggeber vertragswidrig ganz oder teilweise verweigert.

(3) Auch nach einer Kündigung dieses Vertrages oder eines einzelnen Auftragsverarbeitungsverhältnisses gelten die hierin vereinbarten Bestimmungen für die Abwicklung des gekündigten Auftragsverarbeitungsverhältnisses oder dieses Vertrages solange fort, bis diese vollständig rückabgewickelt und die Daten des Auftraggebers auf ihn zurückübertragen sind.

§ 15 Datenschutzbeauftragter des Auftragsverarbeiters

(1) Der Auftragsverarbeiter sichert zu, dass er einen fachkundigen und zuverlässigen Datenschutzbeauftragten bestellt hat. Der nachstehende Mitarbeiter ist beim Auftragsverarbeiter als Beauftragter für den Datenschutz bestellt: Josef Beck

(2) Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

§ 16 Schlussbestimmungen

(1) Ergänzungen und Änderungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für einen etwaigen Verzicht auf dieses Schriftformerfordernis.

(2) Sollte Eigentum des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen.

(3) Es besteht bei den Vertragsparteien Einigkeit darüber, dass „Allgemeine Geschäftsbedingungen" des Auftragsverarbeiters auf diesen Vertrag keine Anwendung finden.

(4) Erweist sich eine Bestimmung dieses Vertrages als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen des Vertrags nicht. Beide Vertragsparteien sind in diesem Falle verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

(5) Sollten Widersprüche zwischen Bestimmungen dieses vorliegenden Dokuments und übrigen Vertragsdokumenten bestehen, gehen die Bestimmungen des vorliegenden Dokuments den übrigen Vertragsdokumenten vor.

(6) Rechtswahl, Gerichtsstandsvereinbarung

Für diesen Vertrag gilt das Recht des Landes, in dem der Auftraggeber seinen Sitz hat, unter Ausschluss der Regelungen des internationalen Privatrechts.

Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist, vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes, der Sitz des Auftraggebers. Der Auftraggeber ist berechtigt, einen Rechtsstreit auch am gesetzlichen Gerichtsstand anhängig zu machen.

(7) Anlage 1 ist wesentlicher Bestandteil dieses Vertrages.

Berlin, 12.09.2018

Ort / Datum

[redacted]

Auftraggeber

Berlin, 18.09.2018

Ort / Datum

[redacted]

Auftragsverarbeiter

Anlage 1

Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung

Die nachfolgenden Maßnahmen zur Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten stellen Mindestanforderungen dar, die eingehalten werden müssen. Weitergehende Maßnahmen, die zu einem höheren Schutzniveau führen, können im Ermessen und zu Lasten des Auftragsverarbeiters eingeführt werden. Maßnahmen, die dem technischen Fortschritt unterliegen, können ebenfalls im Ermessen und zu Lasten des Auftragsverarbeiters eingeführt werden, sofern das geforderte Schutzniveau nicht unterschritten wird.

1. Sicherstellung von Verfügbarkeit und Belastbarkeit

1.1 Verfügbarkeitskontrolle

Durch Brand- und Wasserschäden, Blitzschlag oder Stromausfall oder aber Diebstahl und Sabotage können Datenbestände in Gefahr geraten. Dass in diesen Fällen kein Datenverlust eintritt soll die Verfügbarkeitskontrolle sicherstellen.

Der Schutz vor zufälliger Zerstörung kann hauptsächlich über die Einhaltung entsprechender Brandschutzvorschriften und durch zusätzliche Hardware zur unterbrechungsfreien Stromversorgung und Netzwerksicherheit sichergestellt werden. Mit den entsprechenden Vorkehrungen und Zusatzsoftware können EDV-Systeme beispielsweise im Falle eines plötzlichen Stromausfalles noch so lange weiterbetrieben werden, bis ein kontrolliertes Abschalten möglich ist. Hierdurch können sowohl Datenverlust als auch Hardwareschäden vermieden werden.

Unter die Verfügbarkeitskontrolle fallen aber auch Maßnahmen zur Datensicherung, also die klassischen Backup- und Datenspiegelungslösungen. In welchen Intervallen solche Datensicherungen durchgeführt werden müssen, hängt immer von der Art der Daten, der Veränderungshäufigkeit und der Wichtigkeit der Daten für das Unternehmen ab. Für alle Datensicherungen gilt aber, dass auch die erstellte Sicherung vor Zerstörung und Diebstahl gesichert sein muss. Sicherungskopien dürfen daher nie im gleichen Gebäude oder Brandabschnitt wie das Datenverarbeitungssystem aufbewahrt werden. Vielmehr ist zu empfehlen, die Datensicherung entweder direkt auf einem Server an einem anderen Standort zu erstellen, oder Datenträger mit Datensicherungen entsprechend an einem ausgelagerten Ort aufzubewahren.

Die folgenden Maßnahmen zur Verfügbarkeitskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Es existiert ein Brandschutzkonzept, bestehend aus Brandmeldern, Brandschutztüren und lokalen Feuerlöschern.
Eine unterbrechungsfreie Stromversorgung (USV) für die Server-Systeme ist vorhanden.
Die Serverräume sind klimatisiert.
Es existiert ein schriftliches Datensicherheitskonzept.
Für jedes geschäfts- oder sicherheitskritische System ist entsprechend dem Gefährdungspotential ein redundantes System vorhanden.
Daten werden redundant an 2 Standorten gehalten.
Serverfestplatten werden regelmäßig gespiegelt.
Es erfolgen regelmäßige Tests der erstellten Backups (Test der restore-Funktion).
Virenscanner und Firewall werden regelmäßig kontrolliert und aktualisiert.
Es existiert ein Notfallplan bei Ausfall der Systeme. Dieser wird in regelmäßigen Abständen als Testszenario durchgespielt und die Ergbenisse protokolliert.

1.2 Sicherstellung der Belastbarkeit

Es sind hinreichende Rechen- und Serverkapazitäten einzusetzen, so dass die Funktionsfähigkeit auch bei starkem Zugriff bzw. starker Auslastung gewährleistet ist.

Die folgenden Maßnahmen zur Sicherstellung der Belastbarkeit müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Überwachung der Auslastung anhand von Monitoringdaten
Kapazitätsanpassung bei Überschreitung von vereinbarten Schwellwerten

2. Sicherstellung der Integrität

2.1 Weitergabekontrolle

Die Weitergabekontrolle betrifft im Grunde zwei verschiedene Szenarien. Zum einen wird auf die Sicherung der Übertragungswege von personenbezogenen Daten - gleich ob per Datenträger oder elektronisch - abgezielt. Zum anderen betrifft die Weitergabekontrolle die Revisionsfähigkeit von Datenübermittlungsvorgängen an unternehmensfremde Dritte.

Hinsichtlich des ersten Szenarios müssen Maßnahmen getroffen werden, um zu verhindern, dass Unbefugte während eines Übertragungsvorgangs Zugriff – gleich welcher Art – auf personenbezogene Daten haben. Umfasst werden dabei aber nicht nur die elektronische Übermittlung, sondern beispielsweise auch die Verbringung eines Back-Up-Datenträgers in einen Archivraum. In jedem Fall der Datenübermittlung sind entsprechende Sicherheitsmaßnahmen zu treffen. Dies umfasst auch die Weitergabe von Daten an den Auftragsverarbeiter.

Das zweite Szenario verlangt eine „vorbeugende" Dokumentation darüber, welche Empfänger personenbezogene Daten durch Datenübertragung erhalten sollen. Die Regelung verlangt dabei keine ständige Protokollierung sämtlicher Datenübertragungen, sondern vielmehr soll nur die vorgesehene Übermittlung dokumentiert werden. Für diese Dokumentation müssen alle Übermittlungsadressaten inklusive der an sie zu übermittelnden Datenmenge bezeichnet werden. Des Weiteren müssen die möglichen Übermittlungen in zeitlicher Hinsicht (Beginn und Ende der Übermittlung) überprüfbar sein. Die entsprechenden Dokumentationsunterlagen müssen auch für Dritte einsehbar und in einem entsprechend allgemein lesbaren Format vorhanden sein.

Folgende Maßnahmen zur Weitergabekontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

[illegible]
Die Daten des Auftraggebers werden vom Auftragsverarbeiter nur nach vorheriger schriftlicher Weisung an Dritte weitergegeben.
Es wird durch entsprechende Regelungen (z.B. durch die Einschränkung des Personenkreises, die Datenträger erstellen können und regelmäßige Kontrollen dieser Einschränkung) sichergestellt, dass keine Daten des Auftraggebers unbefugt weitergegeben werden.
Insofern im Rahmen der Auftragsdurchführung Daten weitergegeben werden müssen, erfolgt eine Weitergabe der Daten wenn möglich ausschließlich in anonymisierter Form oder aber es erfolgt eine Verschlüsselung der Daten vor der Weitergabe (z.B. MIME, PGP Standard). Daten werden gemäß dem Stand der Technik verschlüsselt.
Der Transport von Datenträgern erfolgt bei Bedarf durch sichere Transportbehälter (Versiegelung). Bei Ablieferung erfolgt eine Identitätsprüfung des Empfängers.
Es erfolgt eine Dokumentation der Übermittlung.

2.2 Eingabekontrolle

Wie bereits weiter oben erwähnt, ergibt es immer auch Sinn zu protokollieren, wer wann auf welche Daten zugreift, und was verändert wird. Die Maßnahmen

zur Eingabekontrolle sollen genau das sicherstellen. Mit ihnen soll sich jederzeit ermitteln lassen, wer bestimmte Daten erstellt hat, was der Inhalt dieser Daten war und ist und wann die Erstellung bzw. Änderung vorgenommen wurde. So soll ermittelt werden können, wer für falsche oder unvollständige Daten verantwortlich zeichnet. Nicht gespeichert werden dürfen dabei aber die gelöschten oder veränderten Daten an sich. Es obliegt den Unternehmen wie die Identifizierung des „Datenurhebers" umgesetzt wird. Es ist dabei nicht erforderlich, dass sich diese bereits direkt aus dem Datenverarbeitungssystem ergibt. Ausreichend ist beispielsweise auch eine Identifizierungsmöglichkeit über Eingangskontrollbücher oder Schichtpläne.

Zu beachten ist, dass mit der Anfertigung von Eingabeprotokollen eine neue Sammlung personenbezogener Daten entsteht, die als solche behandelt werden muss. Bei einer automatisierten Erstellung sollte daher darauf geachtet werden, dass sich einzelne Einträge auch nur automatisiert wieder ermitteln lassen.

Folgende Maßnahmen zur Eingabekontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

[illegible]
Der Auftragsverarbeiter muss Zugangsregelungen und Benutzerberechtigungen im Einsatz haben, mit denen die Identifizierung aller Benutzer und Datenstationen im System möglich ist.
Aktivitäten auf den Systemen müssen über Protokoll-Funktionen nachvollziehbar sein.
Die entsprechenden Protokolle werden für einen festgelegten Zeitraum aufbewahrt.
Zugriff auf diese Protokolle haben definierte Personen (z.B.: Datenschutzbeauftragte und IT-Sicherheitsbeauftragte). Die Protokolldateien sind gegen unbefugte Nutzung und Veränderung gesichert.

3. Sicherstellung der Vertraulichkeit

3.1 Zutrittskontrolle

Die Zutrittskontrolle verlangt Maßnahmen, die Unbefugten den körperlichen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehren. Es muss also verhindert werden, dass unbefugte Personen überhaupt die Möglichkeit des Zutritts zu Datenverarbeitungsanlagen haben. Die Zutrittskontrolle soll aber nicht nur einen unbefugten Zutritt, sondern auch eine Zerstörung von EDV-Anlagen verhindern.

Die Zutrittsberechtigungen sind daher immer genau festzulegen und zu dokumentieren. Dies gilt insbesondere auch für unternehmensfremde Personen wie

Wartungstechniker (denen immer Begleitpersonen an die Seite gestellt werden sollten) oder das Reinigungspersonal. Zur Zutrittskontrolle gehören aber auch alle Maßnahmen, die ein gewaltsames Eindringen verhindern.

Eine effektive Zutrittskontrolle ist in der Regel nur durch eine Kombination von verschiedenen ineinandergreifenden Maßnahmen möglich.

Folgende Maßnahmen zur Zutrittskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Die Sicherung des Betriebsgeländes erfolgt durch: • Umzäunung • Sichtkontrollen und Gästelisten am Empfang/Pförtner • außerhalb der Betriebszeiten Überwachung durch einen Wachdienst • Betrieb von Überwachungseinrichtungen wie Alarmanlagen und Video-/Monitorüberwachung.
Der Brandschutz wird sichergestellt durch: • Brandschutztüren • lokale Feuerlöscher • Brand- bzw. Rauchmeldern mit Direktaufschaltung zur Feuerwehr.
Schlüssel und andere Türöffnungssysteme (z.B. Magnetkarten) werden ausschließlich personenbezogen ausgegeben und protokolliert.
Es existiert ein mehrstufiges Sicherheits- und Schließkonzept für besonders schützenswerte Räume. Die Schlüsselausgabe erfolgt nur an einen eingeschränkten Personenkreis und wird protokolliert.
Die Serverräume sind durch stets verschlossene Sicherheits- und Brandschutztüren von den übrigen Räumen abgetrennt.
Die TK-Anlage ist von den übrigen Räumen abgetrennt.

3.2 Zugangskontrolle

In Abgrenzung zur „räumlichen" Zutrittskontrolle müssen Maßnahmen der Zugangskontrolle die Benutzung von Datenverarbeitungsanlagen durch unbefugte Personen verhindern. Es muss hier eine Identifikation der Nutzer und Prüfung der Berechtigungen erfolgen, um eine unzulässige Kenntnisnahme oder gar eine Änderung oder Löschung von personenbezogenen Daten zu verhindern.

Folgende Maßnahmen zur Zugangskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Es werden ausschließlich individuelle, persönliche Benutzerkennungen angewendet und keine Gruppenpasswörter genutzt.

Maßnahmen
Es existiert eine systemseitige und mittels Arbeitsanweisung festgelegte Passwortregelung: • Es werden mindestens 8 Zeichen und ein entsprechender Zeichenmix verwendet. • Das Passwort wird regelmäßig gewechselt (z.B. nach 3 Monaten).
Es erfolgt eine systemseitige Einschränkung der Passwortwahl, damit z.B. bereits verwendete Passwörter nicht abwechselnd genutzt werden können.
Es gibt eine systemseitige Zugangssperre bei mehr als 3 Anmeldeversuchen.
Es erfolgt eine systemseitige Bildschirmsperre bei Pausen mit Passwort Aktivierung.
Der Zugang zu den Systemen (An- und Abmeldung) wird protokolliert.
Es existieren verschiedene Berechtigungsstufen und Zuteilung dieser auf die Nutzer.
Es ist eine Firewall und ein Virenscanner installiert. Gemäß Checklisten und Protokollen werden regelmäßige Updates und Sicherheitspatches installiert, um das Schutzniveau hoch zu halten.
Für die IT-Systeme werden Administratoren eingesetzt. Diese nutzen spezielle Passwortkonventionen. Die Administratorenarbeit wird systemseitig protokolliert.
Fernwartung erfolgt unter Verwendung eines Virtual Private Networks (VPN).

3.3 Zugriffskontrolle

Mitarbeiter des Auftragsverarbeiters und Dritte mit entsprechenden Berechtigungen dürfen nur auf Daten zugreifen, die für die Erbringung der Dienstleitung relevant und erforderlich sind. Bei der Zugriffskontrolle geht es daher darum, die berechtigten Zugriffe auf Daten insoweit zu beschränken als es für die zugreifenden Personen möglich und nötig ist.

Die verschiedenen Berechtigungen können dabei den Zugriff auf bestimmte Teile des Netzwerkes, bestimmte Programme und/oder bestimmte Bearbeitungsrechte (Leserechte, Druckrechte, Veränderungsrechte) regeln. Darüber hinaus bietet es sich an, berechtigte Zugriffe zu protokollieren, um später nachvollziehen zu können, wer wann auf welche Daten zugegriffen und diese eventuell verändert hat.

Folgende Maßnahmen zur Zugriffskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Es existiert ein rollenbasiertes Berechtigungskonzept (verschieden Berechtigungsstufen) für die Zugriffe der Mitarbeiter auf Daten. Die Rechteverwaltung erfolgt durch Administratoren.
Die Clear Desk Policy des Auftragsverarbeiters wird eingehalten.
Es erfolgt eine restriktive Rechte-Vergabe auf Basis eines „Need-to-know" Ansatzes.

Maßnahmen
Die Berechtigungsvergabe wird regelmäßig überprüft, protokolliert und die Protokolle werden für einen festgelegt Zeitraum aufbewahrt.
Es erfolgt eine organisatorische Trennung von Administration und Betrieb/Anwendung.
Der Zugang zu den Systemen (An- und Abmeldung) wird protokolliert und die Zugriffsprotokolle werden periodisch ausgewertet.
Insofern externe Datenträger für die Speicherung von Kundendaten genutzt werden, werden diese Datenträger, die Daten des Auftraggebers enthalten, gemäß dem Stand der Technik verschlüsselt. Die Aufbewahrung findet in gesicherten Räumen statt.
Datenschutzgerechte Datenträgerentsorgung. Die physikalische Vernichtung erfolgt gemäß DIN 66399 mindestens in Sicherheitsstufe 3
Die Vernichtung von Ausdrucken mit personenbezogenen Daten des Auftraggebers erfolgt durch entsprechende Aktenvernichter (cross cut).

4. Sicherstellung von Nichtverkettbarkeit durch Zweckbestimmung

4.1 Verwendungszweckkontrolle/Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene personenbezogene Daten müssen natürlich auch getrennt gespeichert und ausgewertet werden. Diesem Erfordernis wird das Datentrennungsgebot gerecht, welches organisatorische und technische Maßnahmen zur Datentrennung verlangt.

Getrennt werden müssen beispielsweise Mitarbeiter- und Kundendaten, oder auch die Daten verschiedener Kunden bei einem Auftragsverarbeiter. Eine physikalische Trennung (verschiedene Datenträger) ist jedoch nicht immer umsetzbar oder wirtschaftlich sinnvoll. Es ist daher ausreichend wenn die Daten logisch getrennt voneinander gespeichert werden. Dafür ist es ausreichend wenn die Daten beispielsweise nur über verschiedene Zugangsdaten erreichbar sind.

Folgenden Maßnahmen zur Trennungskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Sofern keine dedizierten Systeme für genau einen Kunden zum Einsatz kommen, müssen die genutzten Systeme mandantenfähig sein.
Zur Sicherstellung des Produktivbetriebs ist das Entwicklungssystem vollständig von den Produktivsystemen getrennt. Ein Austausch findet ausschließlich im für die Verarbeitung erforderlichen Rahmen und Umfang statt (Programmdateien, Parameterdateien, etc.)

4.2 Pseudonymisierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Folgende Maßnahmen zur Pseudonymisierung müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Anonymisierte Kennungen, welche nur mit Hilfe einer separaten Datenbank auflösbar sind.
Überwiegender Einsatz von Serverkennungen, die Rückschlüsse auf die Funktion verbergen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutz-Management

Das Datenschutz-Management gibt organisatorische Maßnahmen vor, die für die Gewährleistung eines rechtskonformen Umgangs mit personenbezogenen Daten ergriffen werden müssen.

Das Datenschutz-Management besteht im Wesentlichen aus der Audit Funktion (lfd. Bestandsaufnahme existierender Datenschutzprozesse), der Governance Funktion (Steuerung des Datenschutzes) sowie der Awareness Funktion (Aufklärung / Information der Mitarbeiter) und beinhaltet u.a. folgende Prozesse:

- interne Prüfungen vor Beginn neuer Verarbeitungen personenbezogener Daten,
- schriftliche Richtlinien („Datenschutzstrategien") zur Gewährleistung der Grundsätze zur Datenqualität, Unterrichtung, Sicherheit und Betroffenenrechte,
- ständige Aktualisierung von Verarbeitungsverzeichnissen,
- Bestellung eines Datenschutzbeauftragten,
- Durchführung von Mitarbeiterschulungen,

- Beschwerde- und Data-Breach-Management (s. ergänzend Ziffer 5.2).

Folgenden Maßnahmen zum Datenschutz-Management müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet worden und sind gemäß DS-GVO, Artikel 29 und 32 (4) angewiesen, personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten.
Der Auftragnehmer führt jährlich Schulungen durch, um das Datenschutzbewusstsein der eingesetzten Mitarbeiter jährlich zu stärken.
Die technischen und organisatorischen Maßnahmen zum Datenschutz gemäß DS-GVO, Artikel 32, werden im Rahmen der ISO-Zertifizierung regelmäßig überprüft.

5.2 Incident-Response-Management

Es müssen IT-Sicherheitskonzepte und Notfallpläne für das Vorgehen beim Ausfall von IT-Systemen sowie für den Fall schwerwiegender Datenschutzverstöße existieren.

Des Weiteren ist eine abgestufte Meldepflicht von Datenpannen an Aufsichtsbehörden und Betroffene vorgesehen. Grundsätzlich muss jede Datenpanne der zuständigen Aufsichtsbehörde gemeldet werden, es sei denn, dass sie „voraussichtlich nicht zu einem Risiko" des Betroffenen führt. Die Meldung der Datenpanne muss innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde stattfinden. Ein Überschreiten der Frist ist nur in begründeten Fällen möglich. Die Meldungen haben u.a. die Art der Datenpanne, die Kategorien von betroffenen Daten, die Anzahl der Betroffenen und der Datensätze, eine Einschätzung der Folgen für den Betroffenen sowie die Maßnahmen zur Ursachenbeseitigung bzw. zur Schadensminimierung beim Betroffenen zu umfassen.

Es ist daher ein Incident-Response-Management vorzuhalten, dass die vorstehenden Anforderungen erfüllt.

Folgenden Maßnahmen zum Incident-Response-Management müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Auftretende Security Ereignisse werden nach einem „ITIL Best Practice" angelehnten Betriebsverfahren bearbeitet, um möglichst zeitnah einen störungsfreien Betrieb wiederzuer-

Maßnahmen
langen.
Security Incidents werden zeitnah überwacht und analysiert. Abhängig von der Art des Ereignisses nehmen an deren Bearbeitung zuständige und notwendige Service Teams und Spezialisten teil.

6. Datenschutzfreundliche Voreinstellungen

Für IT-Systeme sind sog. „datenschutzfreundliche Voreinstellungen" vorzunehmen. Es werden technische Spezifikationen als Grundmodus abverlangt, die vor allem dem Gebot der Datenminimierung Rechnung tragen. Im jeweiligen IT-System ist die Wahl der Voreinstellungen auf das für den jeweiligen Verarbeitungszweck Erforderliche zu begrenzen.

Das Gebot datenschutzfreundlicher Voreinstellungen erstreckt sich auf

- die Menge der erhobenen personenbezogenen Daten,
- den Umfang ihrer Verarbeitung,
- ihre Speicherfristen und
- ihre Zugänglichkeit (Zugangsbeschränkungen).

Folgenden Maßnahmen zu datenschutzfreundlichen Voreinstellungen müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Die Menge der personenbezogenen Daten wird z. B. dadurch minimiert, dass personenbezogene Daten in Logfiles nur sehr restriktiv eingesetzt werden.
Transparenz in Bezug auf die Funktionen und die Verarbeitung Daten wird dadurch hergestellt, dass dargestellt wird, welche Daten für welche Funktion innerhalb der Software verwendet werden.
Daten werden so früh wie möglich gelöscht oder anonymisiert.
Die Zugriffsmöglichkeiten auf Daten wird auf das notwendige Maß minimiert

6.1 Auftragskontrolle

Die Auftragskontrolle soll sicherstellen, dass sich der Auftragsverarbeiter auch an die Weisungen des Auftraggebers hält und Datenverarbeitung nur innerhalb dieser Weisungen stattfindet. Denn allein die Weisungsgebundenheit führt dazu,

dass eine Weitergabe von Daten an den Auftragsverarbeiter nicht als Weitergabe an Dritte gewertet wird, welche zustimmungsbedürftig wäre.

Die Auftragskontrolle verlangt deshalb nach in Art und Umfang verhältnismäßigen Maßnahmen, welche sicherstellen, dass das Übermitteln, Speichern, Nutzen, Verändern und Löschen personenbezogener Daten nur nach Vorgabe des Auftraggebers beim Auftragsverarbeiter erfolgen kann. Zum einen hat also der Auftragsverarbeiter die Weisungen des Auftraggebers einzuhalten, zum anderen muss der Auftraggeber dafür Sorge tragen, dass seine Weisungen verständlich und umsetzbar sind und auch befolgt werden.

Die Weisungen können dabei in jeder Form erteilt werden, es empfiehlt sich jedoch eine Form zu wählen, die zum einen Irrtümer vermeidet und später ordentliche Nachweise ermöglicht. In der Praxis lassen sich diese Erfordernisse am besten über die Nutzung von Formularen (schriftlich oder elektronisch) bei der Auftragserteilung umsetzen. In den Weisungen sollte immer auch enthalten sein, welche Daten wie übermittelt werden sollen.

Erfolgte Maßnahmen sind sowohl vom Auftraggeber, als auch vom Auftragsverarbeiter ständig auf ihre Umsetzung zu überprüfen und gegebenenfalls zu verbessern.

Folgende Maßnahmen zur Auftragskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Es werden detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung, Nutzung, Wartung, usw. personenbezogener Daten des Auftraggebers, sowie über deren Zweckbindung im Vertrag festgehalten.
Die Erteilung von Weisungen erfolgt in schriftlicher oder elektronischer Form. Mündliche Weisungen sind nur in begründeten Ausnahmefällen zulässig und müssen unverzüglich schriftlich von Auftraggeber bestätigt werden.
Während der Durchführung der beauftragten Dienstleistung erfolgt eine Kontrolle der Auftragsausführung. Für die Kontrolle der Auftragsausführung wird ein gemäß ITIL „Best Practice" beschriebenes Change Vorgehen praktiziert. Dementsprechend ist nur ein zuvor autorisierter Kundenvertreter berechtigt, einen Change freizugeben.
Eine genehmigte Weitergabe an Dritte (Subunternehmer) ist nur zulässig, wenn die Zusammenarbeit in einem entsprechenden Vertrag geregelt ist und die Schutzmaßnahmen des Subunternehmers die gleichen Kriterien wie die des Auftragsverarbeiters erfüllen. Die Subunternehmer werden in regelmäßigen Abständen sowie bei besonderen Vorkommnissen auf die Einhaltung des Schutzniveaus überprüft.