Datenschutzrechtliche Vertragsregelungen nach § 11 BDSG für estos ProCall Mobility Services und die Anbindung der Push-Dienste von Drittanbietern

Stand: 06/2017_v1

Auftraggeber:

Das ist Ihr Unternehmen.

Auftragnehmer:

estos GmbH
Petersbrunner Str. 3a
82319 Starnberg

1. Gegenstand und Dauer der Vereinbarung

1.1. Der Auftrag umfasst Folgendes

- Die **ProCall Mobilitiy Services** ermöglichen ausgewählten Benutzern von ProCall Enterprise die externe Nutzung von ProCall Client Anwendungen durch die Verwendung eines estos Online-Dienstes.
- Anbindung der **Push-Dienste von Drittanbietern** (z.B. Apple Push-Benachrichtigungsdienst, Google Cloud Messaging) an ProCall Enterprise zur Bereitstellung einer Benachrichtigungsfunktion für ProCall Mobile.

Der Auftragnehmer erhebt / verarbeitet / nutzt dabei personenbezogene Daten im Auftrag des Auftraggebers nach § 11 BDSG, oder kann bei Durchführung des Auftrags mit personenbezogenen Daten in Berührung kommen. (z. B. bei Systembetreuung oder Wartung/Fernwartung/§ 11 Abs. 5 BDSG).

1.2. Dauer des Auftrags

Der Vertrag wird auf unbestimmte Zeit geschlossen.

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

2. Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

Das Endanwenderunternehmen betreibt einen ProCall Enterprise Server unter eigener Hoheit, der bestimmte Dienste (z.B. Telefonjournal, Chat, Kontaktsuche) für die Nutzung durch Client Applikationen bereitstellt.

- Im Rahmen der **ProCall Mobility Services** wird eine Verbindung zwischen dem Kundenserversystem und den ProCall Clientanwendungen über einen von estos betriebenen Online-Dienst hergestellt. Dabei werden (personenbezogene) Daten zwischen dem Serversystem und den Clientanwendungen über den Online-Dienst ausgetauscht.
- Zur Anbindung der **Push-Dienste von Drittanbietern** werden (personenbezogene) Daten von dem Kundenserver an einen Online-Dienst von estos weitergegeben, dort verarbeitet und dann an den Push-Dienst des entsprechenden Drittanbieters weitergeleitet. Die Nutzdaten sind zwischen dem Kunden Server und dem Client Ende-zu-Ende verschlüsselt, können also vom estos Online-Dienst nicht gelesen werden. Durch den Online-Dienst werden lesbare Logdateien (z.B. IP-Adressen, Zugriffe) erstellt und persistiert.

2.1. Art der Daten

ProCall Mobility Services

- Kontaktdaten der Mitarbeiter des Endanwenderunternehmens
- Kommunikationsdaten der Mitarbeiter des Endanwenderunternehmens (z.B. Verbindungsdaten)
- Persönliche Kommunikation zwischen Mitarbeitern des Endanwenderunternehmens
- Persönliche Kommunikation zwischen Mitarbeitern des Endanwenderunternehmens und Dritten (über Federation)
- Echtzeitkommunikationsdaten (Audio und Video)

Anbindung der Push-Dienste von Drittanbietern

- Kontaktdaten der Mitarbeiter des Endanwenderunternehmens
- Kommunikationsdaten der Mitarbeiter des Endanwenderunternehmens (z.B. Verbindungsdaten)
- Persönliche Kommunikation zwischen Mitarbeitern des Endanwenderunternehmens

- Persönliche Kommunikation zwischen Mitarbeitern des Endanwenderunternehmens und Dritten (über Federation)

2.2. Kreis der Betroffenen

Betroffen sind Vordergründig alle Mitarbeiter des Endanwenderunternehmens, insbesondere die Nutzer von ProCall Enterprise. Durch die Anbindung von Unternehmensdatenquellen (z.B. CRM-System) können die betroffenen Personengruppen nahezu beliebig erweitert werden.

3. Technische und organisatorische Maßnahmen nach § 9 BDSG

Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt.

Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

Die Datensicherheitsmaßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

Wesentliche Änderungen sind vom Auftragnehmer mit dem Auftraggeber schriftlich vorab abzustimmen.

4. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder zu sperren, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

5. Pflichten des Auftragnehmers

(i.) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(ii.) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(iii.) Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Eingang und Ausgang werden dokumentiert.

(iv.) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

(v.) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

(vi.) An der Erstellung der Verfahrensverzeichnisse des Auftraggebers hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

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

(viii.) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Sicherheitskontrollen vor Ort.

(ix.) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(x.) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit) ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung für Kontrollzwecke des Auftraggebers vertraglich sicher zu stellen.

(xi.) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG bekannt sind. Der Auftragnehmer bestätigt, dass ihm auch folgende datenschutzrechtliche Vorschriften bekannt sind: Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren.

(xii.) Er verpflichtet sich, Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen und dem Auftragnehmer separat vorher mitgeteilt werden (z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, etc.).

(xiii.) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(xiv.) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Weisung oder Zustimmung durch den Auftraggeber erteilen.

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr
Christian Volkmer, Projekt 29 GmbH & Co. KG, Tel.: 0941 29 86 93 0
bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Unterauftragsverhältnisse

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von § 9 BDSG sorgfältig auswählt.

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

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach § 11 BDSG erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig zu überprüfen.

Zurzeit sind für den Auftragnehmer die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten

in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden

7. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich festzulegen.

Der Auftraggeber erteilt alle Aufträge oder Teilaufträge in der Regel schriftlich. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

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

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

7.1. Weisungsberechtigte des Auftraggebers

Weisungsberechtigte Personen des Auftraggebers können dem Auftragnehmer via E-Mail mitgeteilt werden.

7.2. Weisungsempfänger beim Auftragnehmer sind

David Welzmiller, Produktmanagement, +49 8151 36856 151

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

8. Mitteilungspflichten des Auftragnehmers

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42 a BDSG sowie § 15a TMG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42 a BDSG zu unterstützen.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder sofern dies nicht möglich ist, nach vorheriger Abstimmung mit dem Auftraggeber, datenschutzgerecht zu löschen bzw. zu vernichten. In diesem Fall ist die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

10. Haftung

Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

11. Sonstiges

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 unverzüglich zu verständigen.

Für Nebenabreden ist die Schriftform erforderlich.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 zum ADV-Vertrag – Technische und Organisatorische Maßnahmen der Firma estos GmbH

1. Organisation

Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem BDSG eingesetzt.
Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten	Christian Volkmer, Projekt 29 GmbH, Ostengasse 14, 93047 Regensburg, Tel: 0941-2986930
Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden nach §5 BDSG verpflichtet.
Wie stellen Sie sicher, dass die internen Prozesse gemäß den aktuellen Datenschutzbestimmungen ablaufen und wird des regelmäßig geprüft?	Überprüfung (auch unangekündigt) durch den externen DSB.
In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Regelmäßige Schulung durch den externen DSB.
Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Ja, die Verfahren sind im internen Verfahrensverzeichnis dokumentiert.

2. Zutrittskontrolle

Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Alarmanlage in Gebäudeanteil der Firma

Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Sicherungskreise der Alarmanlage. Zutritt nur für Mitarbeiter per dediziertem RFID-Chip. Benachrichtigung von Sicherheitsdienst und bestimmten Mitarbeitern bei Alarm.
Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Gesonderter Sicherungskreis der Alarmanlage mit Zugang nur für Administrationspersonal.
Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.

3. Zugangskontrolle

Wie erfolgt die Vergabe von Benutzerzugängen?	Die Abteilungsleiter bzw. Geschäftsführer melden den Eintritt neuer Mitarbeiter an die Administration. Mitarbeiter erhalten bei Eintritt Active Directory Accounts, die Berechtigungen werden über AD-Gruppen geregelt. (Abteilungs-, Team- oder individuell basierte Zugehörigkeiten)
Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Die Abteilungsleiter bzw. Geschäftsführer sind verpflichtet, relevante Änderungen in Beschäftigungsverhältnissen rechtzeitig der Administration anzuzeigen.
Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Anforderungen zu Benutzerzugängen können nur von den Abteilungsleitern bzw. Geschäftsführern per E-Mail beantragt bzw. genehmigt werden und werden von der Administration per E-Mail bestätigt. Der Verlauf wird über die Mail-Archivierung festgehalten.

Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Administrationszugänge erhalten nur der dedizierte Systemadministrator und Vertretungen aufgrund Genehmigung durch die Geschäftsführung. Alle betreffenden und in Frage kommenden Personen besitzen einen nachweislichen fachlichen IT-Hintergrund mit Erfahrung in der Administration. Sie sind weder temporär noch als externe Mitarbeiter beschäftigt, befinden sich nicht in Probezeit, und wurden auf die Datenschutzerklärung des Unternehmens verpflichtet.
Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Der Zugriff ist über eine verschlüsselte VPN-Verbindung (L2TP) für explizit freigegebene Mitarbeiter möglich. Die Authentifizierung erfolgt über die Active Directory-Anmeldedaten und einen Preshared Key.
4. Zugriffskontrolle	
Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Es existieren keine gemeinsam genutzten Benutzerzugänge. Die Benutzer erhalten ein individuelles Initial-Passwort. Eine Änderung des Passwortes wird bei der ersten Anmeldung technisch erzwungen. Die Mitarbeiter werden bei der Einstellung unterwiesen, sorgsam mit Passwörtern umzugehen und diese nicht anderen Personen zugänglich zu machen.
Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Es werden nur Kennwörter akzeptiert, die keinen Teil des Benutzer-Logons oder –Namens darstellen, 3 aus 4 verschiedenen Zeichenklassen enthalten, und mind. 8 Zeichen lang sind.

Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Durch Gruppenrichtlinien wird ein Wechsel des Passworts nach 60 Tagen erzwungen oder der Zugriff gesperrt. Das neue Passwort darf nicht einem der drei vorherigen entsprechen.
Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Zugriffsfreigaben erfolgen User- und Gruppen-basiert für die mit der Verarbeitung betrauten Personen. Die Systeme sind Passwortgeschützt. Arbeitsplätze werden automatisch bei Inaktivität gesperrt. Die Mitarbeiter sind unterwiesen, bei Verlassen des Arbeitsplatzes ihre Arbeitsplätze zu verlassen und keine sichtbaren bzw. frei zugängliche personenbezogene Daten zu hinterlassen.
Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch 3.1. Die Geschäftsführung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur.
Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Über die Access Control Lists in den Systemen.
Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Sporadische Durchsicht der Systemprotokolle durch die Geschäftsführung.
Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter, ausschließlich die Geschäftsführung
5. Weitergabekontrolle	
Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Die Weitergabe erfolgt über verschlüsselte Kanäle und/oder die Verschlüsselung der Daten selbst. Eine Zustellung oder Bekanntgabe von Zugangsdaten erfolgt nur an den vorgesehen Empfänger.

Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Ein Versenden per E-Mail oder Bereitstellung per Internet erfolgt über Server mit Transportverschlüsselung (TLS). Die Verschlüsselung von Daten erfolgt auf Datenträgerbasis über Microsoft Bitlocker und/oder über verschlüsselte ZIP-Archive (AES-256).
Wie wird die Weitergabe personenbezogener Daten dokumentiert?	n/a
Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Dies wird im Rahmen der Kontrollen zu 4.7 mit geprüft.

6. Eingabekontrolle

Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Zugriffs-Logs der Server und Systeme.
Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Zugriffs-Logs der Applikationen.
Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?	n/a
Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Die Datenverarbeitung von Unterauftragnehmern erfolgt mit eindeutigen Auftragsdefinitionen und einer formalisierten Auftragserteilung.
Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung § 11 BDSG, Bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.

7. Verfügbarkeitskontrolle

Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?	Die Server- und Stromversorgungssysteme der Verarbeitungsanlage sind redundant ausgelegt, um einem Ausfall vorzubeugen.
Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Die Backup-Datenträger werden in einem entsprechenden Panzerschrank aufbewahrt. Backup-Sätze werden turnusmäßig extern durch die Geschäftsführung ausgelagert.
Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Betriebssystem-Sicherheitsupdates und Antiviren-Software und –Definitionen werden zentral automatisiert ausgerollt und aktualisiert. Antiviren- und Firewall-Lösungen werden auf den Client- und Serversystemen eingesetzt. Eingehende Mails werden vor Zustellung durch den Mail-Transport-Server auf Schädlinge und gefälschte Absenderdaten geprüft.
Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Die anfallenden Datenträger werden zentral durch die IT-Abteilung entsorgt. Funktionsfähige Datenträger werden entsprechend geeigneter Methoden sicher gelöscht. (z.B. mehrfaches Überschreiben) Nicht funktionsfähige Datenträger werden physikalisch vernichtet.

8. Trennungskontrolle

Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Zur Trennung der Daten wird ein dezidiertes Rechtesystem eingesetzt.