Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Gültig ab: 01.01.2026

zwischen

Organisation und Rechtsform

Straße Nr.

PLZ, Stadt

Land

- im Folgenden „**Auftraggeber**“ genannt –

Und

Acture Germany GmbH
Kronenstraße 71
10117 Berlin
Deutschland

- Im Folgenden „**Auftragnehmer**“ genannt –

- gemeinsam als „**Vertragsparteien**“ bezeichnet –

1. Geltungsbereich und Definitionen

1.1. Dieser Auftragsverarbeitungsvertrag (im Folgenden „AVV“) regelt die Rechte und Pflichten der Vertragsparteien im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Dieser AVV ist so konzipiert, dass er den Bestimmungen der geltenden Datenschutzgrundverordnung (im Folgenden „DSGVO“), dem Bundesdatenschutzgesetz und den einschlägigen Landesdatenschutzgesetzen gerecht wird.

1.2. Sofern in diesem AVV der Begriff „Leistungsvereinbarung“ verwendet wird, wird darunter der separate Vertragsschluss zwischen Auftragnehmer und Auftraggeber verstanden, der durch den Abschluss eines Nutzungsvertrags - gemäß der Allgemeinen Geschäftsbedingungen („AGB“) des Auftragnehmers - entsteht.

1.3. Sofern in diesem AVV der Begriff „Software“ benutzt wird, wird darunter die webbasierte Software des Auftragnehmers verstanden. Je nach Leistungsvereinbarung zwischen Auftragnehmer und Auftraggeber werden über die Software folgende Leistungspakete zur Verfügung gestellt:

1.3.1. **Care**: Webanwendung für Mitarbeiterunterstützung, insbesondere um die Beschäftigten des Auftraggebers bei privaten und beruflichen Anliegen zu unterstützen und um die EU-Hinweisgeberrichtlinie umzusetzen.

1.3.2. **Discover**: Webanwendung für Mitarbeiterbefragungen, insbesondere um die Gefährdungsbeurteilung psychischer Belastungen (GBU-Psyche) durchzuführen.

1.4. Dieser AVV findet nur auf solche Tätigkeiten Anwendung, bei denen der Auftragnehmer, Beschäftigte des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers gemäß der Leistungsvereinbarung im Sinne von Art. 28 DSGVO verarbeiten. Die wechselseitige Übermittlung personenbezogener Daten zwischen den Vertragsparteien sowie die Mitarbeiterunterstützung durch Ansprechpersonen des Auftragnehmers sind ausdrücklich nicht Gegenstand dieses AVV; die Verarbeitung personenbezogener Daten erfolgt insoweit jeweils in eigener, alleiniger Verantwortung der Vertragsparteien.

1.5. Ergibt ein von einer der Vertragsparteien in Auftrag gegebenes unabhängiges Rechtsgutachten oder erhält mindestens eine der Vertragsparteien eine Anordnung der zuständigen Datenschutzaufsichtsbehörde, dass eine Anpassung dieses AVV und/oder der Verarbeitungstätigkeiten und/oder der den betroffenen Personen zur Verfügung gestellten Informationen erforderlich ist, um die Einhaltung der DSGVO zu gewährleisten, verpflichten sich die Vertragsparteien, die erforderlichen Anpassungen unverzüglich vorzunehmen.

1.6. Soweit nicht anders definiert, sind die in diesem AVV verwendeten Begriffe entsprechend ihrer Definition in der DSGVO zu verstehen.

2. Gegenstand, Spezifizierung, Ort und Dauer der Auftragsverarbeitung

2.1. Gegenstand, Umfang, Art und Zweck der Datenverarbeitung ergeben sich aus diesem AVV und der Leistungsvereinbarung. Eine Auftragsverarbeitung nach Maßgabe dieses AVV liegt danach hinsichtlich der folgenden Verarbeitungen personenbezogener Daten vor:

2.1.1. Hosting der Software einschließlich des Zugangsmanagements (Dashboard-Zugänge)

2.1.2. Support für Anwender:innen der Software

2.1.3. Bereitstellung der technischen Infrastruktur für die Kontaktaufnahme mit Ansprechpersonen des Auftraggebers

2.2. Unabhängig von dem vereinbarten Leistungspaket aus Ziffer 1.3 sind folgende Datenarten bzw. -kategorien regelmäßig Gegenstand der Verarbeitung:

2.2.1. Personalstammdaten von Ansprechpersonen und Administratoren des Auftraggebers (insb. Name, Position, Telefonnummer, E-Mail-Adresse)

2.2.2. Profilfoto von Ansprechpersonen und Administratoren des Auftraggebers

2.2.3. Allgemeine und besondere Personendaten von Beschäftigten des Auftraggebers, die diese - im Rahmen von Umfrageteilnahmen, Beratungsanfragen oder zwecks Abgabe von Hinweisen - gemäß Art. 6 Abs. 1 lit.

a und Art. 9 Abs. 2 lit. a DSGVO übermitteln (insb. Angaben zu Anstellungsverhältnis, Dauer der Unternehmenszugehörigkeit, Abteilung, Alter, Geschlecht, religiösen oder weltanschaulichen Überzeugungen, Familienstand, politischer Meinung oder sexueller Orientierung)

2.3. Unabhängig von dem vereinbarten Leistungspaket aus Ziffer 1.3 umfassen die Kategorien der durch die Verarbeitung betroffenen Personen regelmäßig:

2.3.1. Freie und angestellte Beschäftigte des Auftraggebers oder, falls zutreffend, eines mit ihm verbundenen Unternehmens oder sonstiger Vertragspartner des Auftraggebers, soweit von den Vertragsparteien vereinbart.

2.3.2. Ehemalige freie und angestellte Beschäftigte des Auftraggebers oder, falls zutreffend, eines mit ihm verbundenen Unternehmens oder sonstiger Vertragspartner des Auftraggebers, soweit von den Vertragsparteien vereinbart.

2.4. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt.

2.5. Die Verlagerung des Dienstes in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Sollten diese Anforderungen erfüllt sein, müssen jedoch wichtige datenschutzrechtliche Gründe vorliegen, um die Zustimmung zu verweigern.

2.6. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung, sofern sich aus den Bestimmungen dieses AVV nicht darüberhinausgehende Verpflichtungen ergeben. In letzterem Fall endet dieser AVV mit Wegfall der über die Leistungsvereinbarung hinaus bestehenden Pflichten.

2.7. Bei Widersprüchen zwischen der Leistungsvereinbarung oder den AGB und diesem AVV geht der AVV in datenschutzrechtlichen Belangen als speziellere Regelung vor.

2.8. Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

3. Vertraulichkeit

3.1. Der Auftragnehmer gewährleistet die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29 und 32 Abs. 4 DSGVO.

3.2. Der Auftragnehmer setzt bei der Durchführung der für die Auftragsverarbeitung erforderlichen Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers, der Leistungsvereinbarung und der in diesem AVV eingeräumten Befugnisse verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO wegen eines wichtigen öffentlichen Interesses verbietet.

4. Pflichten des Auftraggebers

4.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf den in dieser Vereinbarung geregelten Gegenstand, Umfang, Art und

Zweck der Datenverarbeitung, die Beschreibung der betroffenen Daten gemäß Ziffer 2 und die Wahrung der Betroffenenrechte.

4.2. Bei der Beurteilung eines angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den Risiken für die betroffenen Personen gebührend Rechnung.

4.3. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.

4.4. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen dieses AVV anfallende Datenschutzfragen.

4.5. Weitere Rechte und Pflichten des Auftraggebers ergeben sich aus den nachfolgenden Regelungen dieses AVV und der DSGVO sowie den dazugehörigen gesetzlichen Bestimmungen.

5. Weisungen

5.1. Der Auftragnehmer - und jede ihm unterstellte Person - darf die personenbezogenen Daten nur im Rahmen von Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne von Art. 28 Abs. 3 S. 2 lit. a DSGVO oder einer anderen vorrangigen Rechtsvorschrift vor. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Leistungsvereinbarung und der AVV stellen die abschließenden Weisungen des Auftraggebers (in Bezug auf die Datenverarbeitung) zum Zeitpunkt des Abschlusses dieses AVV dar. Weitere Weisungen sind dem Auftraggeber vorbehalten, werden jedoch gemäß Ziffer 5.3 behandelt. Der Auftragnehmer nimmt Weisungen des Auftraggebers in schriftlicher Form sowie über die hierfür vom Auftragnehmer angebotenen elektronischen Formate entgegen. Mündliche Weisungen sind nur in Eilfällen gestattet und durch den Auftraggeber unverzüglich schriftlich oder in einem hierfür vom Auftragnehmer angebotenen elektronischen Format zu bestätigen.

5.2. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen einschlägige Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber nach Überprüfung bestätigt oder abgeändert wurde. Für aus bestätigten Weisungen entstehende Schäden jedweder Art haftet der Auftraggeber dem Auftragnehmer im Innenverhältnis voll und stellt den Auftragnehmer gegen Ansprüche Dritter auf erste Anforderung frei. Bei andauerndem Dissens einigen sich die Parteien darauf, die für den Auftraggeber zuständige Aufsichtsbehörde zur Entscheidung hinzuzuziehen.

5.3. Sind die Weisungen des Auftraggebers nicht vom vertraglich vereinbarten Leistungsumfang umfasst, werden diese als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisungen nicht zumutbar, so ist der Auftragnehmer berechtigt, die Weisungen abzulehnen. Für den Fall, dass der Auftraggeber dennoch auf den Weisungen besteht, steht dem Auftragnehmer ein Sonderkündigungsrecht zu und er kann die Verarbeitung beenden und die Leistungsvereinbarung jederzeit mit sofortiger Wirkung kündigen.

5.4. Der Auftraggeber benennt die zur Erteilung von Weisungen ausschließlich befugten Personen innerhalb der Software oder, sofern dies innerhalb der Software nicht möglich ist, per E-Mail an folgende Adresse: datenschutz@acture.eu. Für den Fall, dass keine weisungsbefugte Person benannt wird, sind ausschließlich vertretungsberechtigte natürliche Personen des Auftraggebers zur Erteilung von Weisungen berechtigt. Der

Auftragnehmer kann die Ausführungen von Weisungen so lange aussetzen, bis der Auftraggeber einen Nachweis der Vertretungsberechtigung erbracht hat.

6. Pflichten des Auftragnehmers

6.1. Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses AVV gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung nachfolgender Vorgaben.

6.2. Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Internetseite des Auftragnehmers (www.acture.de/legal) abrufbar.

6.3. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

6.4. Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten aus dieser Auftragsverarbeitung beim Auftragnehmer ermittelt, es sei denn, der Auftragnehmer ist gesetzlich oder behördlich verpflichtet, eine Mitteilung zu unterlassen.

6.5. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, unterstützt ihn der Auftragnehmer auf Anfrage nach besten Kräften.

6.6. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die TOM, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

6.7. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage Dokumente zur Nachweisbarkeit der getroffenen TOM bereit.

6.8. Der Auftraggeber ist berechtigt, die Einhaltung der Pflichten aus dem AVV, der TOM sowie der datenschutzrechtlichen Vorschriften nach Vereinbarung mit dem Auftragnehmer - unter Berücksichtigung eines mindestens 14-tägigen Vorlaufs - zu dessen üblichen Geschäftszeiten selbst zu kontrollieren oder durch im Einzelfall zu benennende Prüfer kontrollieren zu lassen. Dazu kann der Auftraggeber unter anderem die maßgeblichen Gebäude und Einrichtungen des Auftragnehmers besichtigen, Auskünfte einholen oder Einsicht in die eigenen Daten unter Rücksichtnahme auf die berechtigten Interessen des Auftragnehmers nehmen. Für Kontrollen, die aufgrund eines Sicherheitsvorfalls bzw. eines mehr als unwesentlichen Verstoßes gegen die Vorschriften zum Schutz personenbezogener Daten oder Festlegungen dieses AVV erforderlich werden (im Folgenden „anlassbezogene Vor-Ort-Kontrolle“), ist die Anmeldefrist aus Satz 1 auf einen angemessenen Zeitraum verkürzt oder entfällt ganz. Weiterhin unterliegen anlassbezogene Vor-Ort-Kontrollen nicht den Einschränkungen der Ziffern 6.10. – 6.11. dieses AVV.

6.9. Der Auftragnehmer darf die Zustimmung zur Prüfung davon abhängig machen, dass sich der Prüfer einer angemessenen Verschwiegenheitserklärung gegenüber Dritten mit Ausnahme des Auftraggebers und der Aufsichtsbehörden unterwirft. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen oder liegt ein anderer begründeter Fall vor, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

6.10. Im Rahmen dieser Ziffer 6 ist der Auftragnehmer lediglich zur Duldung und Mitwirkung bei einer anlasslosen Vor-Ort-Kontrolle pro Kalenderjahr verpflichtet. Der Aufwand einer anlasslosen Vor-Ort-Kontrolle ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6.11. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Insbesondere ermöglicht der Auftragnehmer anlasslose Vor-Ort-Kontrollen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

7. Technische und organisatorische Maßnahmen (TOM)

7.1. Der Auftragnehmer hat die Umsetzung der im Vorfeld des Vertragsschlusses dargelegten und erforderlichen TOM vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsverarbeitung, zu dokumentieren und dem Auftraggeber zur Prüfung bereitzuhalten.

7.2. Der Auftragnehmer hat die Sicherheit der Verarbeitung gemäß Art. 28 Abs. 3 lit. c und 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die TOM zum Zeitpunkt des Vertragsschlusses können Anhang 3 dieses AVV entnommen werden. Die jeweils aktuell geltenden TOM sind über die Internetseite des Auftragnehmers (www.acture.de/legal) abrufbar.

7.3. Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

8. Unterauftragsverhältnisse

8.1. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung, die Inanspruchnahme von Telekommunikationsdienstleistungen, Benutzerservice oder Kundenbeziehungsmanagement sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit gemäß einschlägigen Rechtsvorschriften sicherzustellen, bleibt unberührt.

8.2. Die Beauftragung von Unterauftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten ist grundsätzlich nur mit Genehmigung des Auftraggebers gestattet. Die Liste der Unterauftragnehmer zum Zeitpunkt des Vertragsschlusses kann Anhang 2 dieses AVV entnommen werden und gilt als erteilt. Die jeweils aktuelle Liste der Unterauftragnehmer kann auf der Internetseite des Auftragnehmers (www.acture.de/legal) abgerufen werden.

8.3. Der Auftraggeber erteilt dem Auftragnehmer ferner die allgemeine Genehmigung, weitere Unterauftragnehmer unter Berücksichtigung von Ziffer 2.4 in Anspruch zu nehmen. Der Auftragnehmer informiert den Auftraggeber in Textform durch aktive Mitteilung (bspw. per E-Mail), wenn er die Hinzuziehung weiterer oder die Ersetzung bestehender Unterauftragnehmer beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben, wobei dies nicht ohne wichtigen datenschutzrechtlichen Grund erfolgen darf. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 14 Tagen nach Bereitstellung der Information über die Änderung gegenüber dem Auftragnehmer in Textform zu erheben an: datenschutz@acture.eu. Im Falle des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die Leistung gegenüber dem Auftraggeber innerhalb von 4 Wochen nach Zugang des Einspruchs einstellen und die Leistungsvereinbarung fristlos und mit sofortiger Wirkung kündigen. Die Auslagerung der Daten darf frühestens ab dem Ablauf der Einspruchsfrist und nur dann erfolgen, wenn der Auftraggeber keinen Einspruch einlegt. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden ist erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Unterauftragnehmer im Sinne von Ziffer 8.1. eingesetzt werden sollen. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers in Textform.

8.4. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf die Unterauftragnehmer zu übertragen und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 - 4 DSGVO mit diesen abzuschließen. Insbesondere gewährleistet der Auftragnehmer, dass die TOM der Unterauftragnehmer dem Schutzniveau der TOM aus Ziffer 7 dieses AVV genügen.

8.5. Eine Vor-Ort-Kontrolle bei den Unterauftragnehmern kann durch beide Vertragsparteien erfolgen. Unter den gleichen Voraussetzungen wie in Ziffer 6.11. dieses AVV kann eine Vor-Ort Kontrolle durch den Nachweis einer datenschutzkonformen Verarbeitung ersetzt werden. Der Auftragnehmer gewährt dem Auftraggeber das Recht, Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der Verpflichtungen dieses Vertrages zu erhalten, wobei der Auftragnehmer dies davon abhängig machen kann, dass die Unterauftragnehmer dies - beispielsweise durch den Abschluss einer Vertraulichkeitsvereinbarung - ermöglichen.

9. Betroffenenrechte

9.1. Richtet sich ein Betroffener an den Auftragnehmer mit einer Forderung aus Kapitel III der DSGVO im Hinblick auf die Rechte der betroffenen Person, dann wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist. Weiterhin leitet der Auftragnehmer den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter.

9.2. Unbeschadet Ziffer 9.1 gilt, dass der Auftragnehmer eine umfassende Selbstverwaltung der Daten sowie den autonomen Zugriff, die Bearbeitung und Überprüfung der verarbeiteten Daten durch jeden Mitarbeiter oder Administrator des Auftraggebers, im Rahmen der zugewiesenen Zugriffsrechte, ermöglicht. Sofern es also um die Wahrung der Betroffenenrechte aus Kapitel III der DSGVO geht, ist der Auftraggeber in erster Linie selbst in der Lage und verantwortlich, dem Verlangen eines Betroffenen nachzukommen.

9.3. Sollte trotz der Möglichkeit einer solchen Selbstverwaltung zusätzlich die Unterstützung seitens des Auftragnehmers erforderlich sein, dann wird dieser den Auftraggeber bei der Pflicht zur Beantwortung von

Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nach Möglichkeit unterstützen.

9.4. Der Auftragnehmer haftet nicht, sofern das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird und dies einzig von diesem verschuldet ist.

10. Informations- und Mitwirkungspflichten

10.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und vorherigen Konsultationen, sofern notwendig. Hierzu gehören u.a.:

10.1.1. die Verpflichtung, Verletzung des Schutzes personenbezogener Daten durch den Auftragnehmer, Beschäftigte des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer unverzüglich an den Auftraggeber im Sinne von Art. 33 Abs. 2 DSGVO zu melden.

10.1.2. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung, sofern notwendig. Diesem kann der Auftragnehmer dadurch nachkommen, dass er dem Auftraggeber auf Anforderung die erforderlichen Angaben und Dokumentationen zur Verfügung stellt.

10.1.3. die Unterstützung des Auftraggebers im Rahmen von Konsultationen mit der Aufsichtsbehörde vor der Verarbeitung.

10.1.4. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

10.2. Für Unterstützungsleistungen gemäß Ziffer 10.1.2, 10.1.3 und 10.1.4 kann der Auftragnehmer eine angemessene Vergütung verlangen.

11. Herausgabe und Löschung von Daten

11.1. Mit Beendigung der Auftragsverarbeitung hat der Auftragnehmer die eingebrachten personenbezogenen Daten gemäß den nachfolgenden Ziffern herauszugeben. In der Regel ist die Auftragsverarbeitung mit Vertragsende der Leistungsvereinbarung beendet. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

11.2. Der Auftragnehmer ist verpflichtet, die eingebrachten personenbezogenen Daten für einen Zeitraum von 30 Tagen nach Vertragsende aufzubewahren. Der Auftraggeber ist berechtigt, jederzeit in Textform bis zum Ablauf dieser Frist die Herausgabe in einem maschinenlesbaren Format oder Löschung der gespeicherten personenbezogenen Daten zu verlangen bzw., sofern möglich, diese direkt aus der Software herunterzuladen.

11.3. Erteilt der Auftraggeber dem Auftragnehmer eine verbindliche Löschungsweisung in Textform, so ist der Auftragnehmer berechtigt, auch vor Ablauf der Aufbewahrungsfrist gemäß Ziffer 11.2 die Datenlöschung durchzuführen. Hiervon ausgenommen sind lediglich die Daten, zu deren Aufbewahrung der Auftragnehmer gesetzlich verpflichtet ist.

11.4. Sollte der Auftraggeber bis zum Ablauf der Frist gemäß Ziffer 11.2 weder die herauszugebenden Daten angefordert noch die Löschung dieser verlangt haben, ist der Auftragnehmer verpflichtet, diese Daten zu löschen.

12. Abschließende Bestimmungen

12.1. Die Annahme/Bestätigung des Vertragsschlusses durch den Auftragnehmer kann in einem elektronischen Format im Sinne von Art. 28 Abs. 9 DSGVO erfolgen.

12.2. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Dies gilt insbesondere auch für die Inhalte dieses AVV sowie alle im Rahmen der datenschutzrechtlichen Prüfung zur Verfügung gestellten Dokumente, Nachweise etc. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

12.3. Änderungen und Ergänzungen dieses AVV und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - sind gemäß DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann, einschließlich des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Die Parteien einigen sich darauf, dass Anpassungen des Vertrags oder neue Verträge in einem elektronischen Format im Sinne von Art. 28 Abs. 9 DSGVO zu schließen sind.

12.4. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.

12.5. Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten ausgeschlossen.

12.6. Es gilt das Recht der Bundesrepublik Deutschland. Die Anwendung des UN-Kaufrechts (CISG) ist ausgeschlossen.

12.7. Für alle Streitigkeiten im Zusammenhang mit diesem AVV wird, sofern zulässig, der Sitz des Auftragnehmers als ausschließlicher Gerichtsstand vereinbart.

12.8. Dieser AVV ersetzt alle vorherigen oder gleichzeitigen Zusicherungen, Absprachen, Vereinbarungen, Verträge oder Mitteilungen zwischen dem Auftraggeber und dem Auftragnehmer, ob schriftlich oder mündlich, in Bezug auf den Gegenstand dieses AVV. Die jeweils geschlossenen Leistungsvereinbarungen bleiben hiervon unberührt.

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

[Unterschriftenseite auf der folgenden Seite]

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anhang 1: Liste der Unterauftragnehmer

Die Acture Germany GmbH hat die folgenden Unterauftragnehmer zur Durchführung der Auftragsverarbeitung auf der Acture Plattform beauftragt:

Name	Adresse	Zweck	Serverstandort
Open Telekom Cloud	T-Systems International GmbH Hahnstraße 43d 60528 Frankfurt am Main Deutschland	Hosting der Server zum Betrieb der Software und Versand von (transaktionalen) E-Mails	Magdeburg, Deutschland
Edudip	edudip GmbH Jülicher Str. 306 52070 Aachen Deutschland	Anbieten von virtuellen Live-Events in Form von Videokonferenzen	Frankfurt, Deutschland
3Q	3Q GmbH Belfortstr. 5 81667 München Deutschland	Bereitstellung von Video- und Audiodateien	Nürnberg, Deutschland
Confrere	Confrere AS Dovresvingen 6b 1184 Oslo Norwegen	Bereitstellung von Videoberatungen	Dublin, Irland

Anhang 2: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftraggeber als “Verantwortlicher” sowie Acture als “Auftragsverarbeiter” haben nach Art. 32 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Der Auftraggeber ist dabei für die Identifizierung und Umsetzung eigener geeigneter Maßnahmen gemäß Art. 24 DSGVO selbst verantwortlich.

Im Folgenden sind diejenigen Maßnahmen dargelegt, welche Acture selbst zur Gewährleistung der Sicherheit der Verarbeitung getroffen hat. Sofern notwendig, werden auch entsprechende Maßnahmen relevanter Unterauftragnehmer, insbesondere in Bezug auf physische Sicherheit der Infrastructure as a Service-Provider sowie Rechenzentrumsbetreiber, aufgeführt und entsprechend gekennzeichnet bzw. entsprechend darauf verwiesen.
Acture hat die folgenden technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO zur Gewährleistung von Verschlüsselung und Pseudonymisierung, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit sowie entsprechende Verfahren zur Überprüfung implementiert. Die Maßnahmen sind in der nachfolgenden Tabelle aufgelistet und dokumentiert.

1. Vertraulichkeit	
1.1. Zutrittskontrolle	
Elektronische Türsicherung	Die Eingangstüren zu den Räumlichkeiten von Acture sind grundsätzlich verschlossen und elektronisch gesichert. Eine Öffnung der Türen erfolgt über einen personengebundenen elektronischen Schlüssel.
Kontrollierte Schlüsselvergabe	Es erfolgt eine zentrale, dokumentierte Schlüsselvergabe an die Beschäftigten von Acture. Diese elektronischen Schlüssel könnten zentral von der Geschäftsführung bzw. Personalabteilung deaktiviert werden.
Beaufsichtigung und Begleitung von Fremdpersonen	Ein Zutritt externer Dienstleister und sonstiger Fremdpersonen darf nur durch vorige Autorisierung und Begleitung durch Beschäftigte von Acture erfolgen.
Sicherung von Räumlichkeiten mit erhöhtem Schutzbedarf	Räumlichkeiten oder Schränke mit erhöhtem Schutzbedarf, beispielsweise Schrank mit Vertragsunterlagen, werden grundsätzlich nach Verlassen oder Nutzung verschlossen. Ein Zutritt zu diesen Räumlichkeiten wird nur autorisiertem Personal gewährt.
Geschlossene Türen und Fenster	Mitarbeiter sind organisatorisch dazu angewiesen, Fenster und Türen außerhalb der Bürozeiten geschlossen bzw. verschlossen zu halten.
Physische und umgebungsbezogene Sicherheit der Server-Systeme in den Rechenzentren	Acture setzt ausschließlich Server-Systeme von Rechenzentrumsbetreibern ein, die eine gültige Zertifizierung nach ISO/IEC 27001 besitzen und demnach entsprechende technische und organisatorische Maßnahmen zur physischen und umgebungsbezogenen Sicherheit umsetzen, bspw.:

	- Das Rechenzentrum und die dort verwendeten Systeme sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind. - Das Rechenzentrum selbst ist durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern. - Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. - Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde. - Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet. - Zutritt zu sensiblen Bereichen wird zusätzlich durch Videoüberwachung überwacht. - Ausgebildete Sicherheitskräfte bewachen das Rechenzentrum und die unmittelbare Umgebung 24 Stunden am Tag, 7 Tage die Woche
1.2. Zugangskontrolle	
Verwendung von Authentifizierungsverfahren	Zugänge, die den Zugriff auf personenbezogene Daten ermöglichen, erfolgen stets über verschlüsselte Protokolle: SSH, SSL/ TLS, HTTPS oder vergleichbare Protokolle. **Authentifizierungsverfahren IT-System/Laptop** - Authentifizierung mit Benutzername und Passwort **Authentifizierungsverfahren Kunden-System** (Kunden-System = Zugang für Administratoren und Nutzer des Auftraggebers) - Authentifizierung mit Benutzername und Passwort - Selbst gewähltes Passwort (mind. 8 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen; Speicherung via Bcrypt-Hash, Einhaltung technisch erzwungen) - Zurücksetzen des Passworts via E-Mail Reset-Link - Sperrung des Accounts nach fünf fehlgeschlagenen Login-Versuchen **Authentifizierungsverfahren Admin-System** (Admin-System = Zugang zu Kunden-Systemen via Benutzeroberfläche für Beschäftigte im Bereich Kundenservice sowie Produktentwicklung von Acture) - Authentifizierung mit Benutzername und Passwort - Selbst gewähltes Passwort (mind. 12 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen; Speicherung via Bcrypt-Hash, Einhaltung technisch erzwungen, regelmäßige Änderung des Passworts erzwungen) - Zurücksetzen des Passworts via E-Mail Reset-Link - Sperrung des Accounts nach fünf fehlgeschlagenen Login-Versuchen **Authentifizierungsverfahren Server-/Datenbank-System** (Server-/Datenbank-System = Zugang auf die gespeicherten Daten durch Produktentwicklung des Auftragnehmers) - Administrative Zugriffe erfolgen über VPN und/oder SSH
Benennung von Support- und Weisungsberechtigten	Der Auftraggeber kann Support- und Weisungsberechtigte bestimmen, welche Acture Weisungen entsprechend des Auftragsverarbeitungsvertrages erteilen

und entsprechende Authentifizierung	können. Die Zuordnung zu einem Support- und Weisungsberechtigten erfolgt dabei über die von Acture angegebenen Kontaktdaten (bspw. Name, E-Mail-Adresse, Telefonnummer, Benutzerkennung). Das Kundenservice-Team von Acture ist dazu angehalten, ausschließlich Weisungen von den benannten Personen anzunehmen bzw. Auskünfte zu erteilen und deren Identität im Vorfeld entsprechend zu überprüfen.
Verwendung sicherer Passwörter	Bei der Vergabe und regelmäßigen Aktualisierung von sicheren Passwörtern sind die Maßgaben des BSI IT Grundschutz oder anderer äquivalenter, anerkannter Sicherheitsstandards für den Acture Account sowie für die Laptops, Computer oder sonstige mobile Endgeräte zu berücksichtigen (mind. 12 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, regelmäßiger Wechsel des Kennwortes).
Verbot der Weitergabe von Passwörtern und Nutzung von „Shared Accounts“	Sowohl für Kunden als auch für Beschäftigte von Acture gilt das Verbot der Weitergabe von Passwörtern für die Nutzung von Acture sowie die Nutzung von sogenannten „Shared Accounts“ für den Zugang zu Kunden-, Admin- und administrativen Systemen (d.h. ausschließliche Nutzung persönlicher und individueller User Logins).
Automatische Sperrung bei Inaktivität	Laptops der Beschäftigten von Acture werden bei Nichtbenutzung vom Benutzer mit Passwortschutz gesperrt. Zusätzlich wird eine automatische Bildschirmsperre mit Passwortschutz nach 15 Minuten Inaktivität eingerichtet. Kunden von Acture sind dazu angehalten, vergleichbare Maßnahmen zur Sperrung bei Inaktivität zu treffen. Der Auftraggeber hat dafür Sorge zu tragen.
Einsatz von Anti-Viren-Software	Laptops der Beschäftigten von Acture sind mit einer dem Stand der Technik entsprechenden und aktuell gehaltenen Anti-Viren-Software auf allen betrieblichen oder betrieblich genutzten IT-Systemen ausgestattet. Es dürfen grundsätzlich keine Rechner ohne residenten Virenschutz betrieben werden, es sei denn, es sind andere äquivalente Sicherheitsmaßnahmen nach dem Stand der Technik getroffen oder ein Risiko besteht nicht. Vorgegebene Sicherheitseinstellungen dürfen nicht deaktiviert oder umgangen werden.
„Clean Desk Policy“	Beschäftigte von Acture sind dazu angehalten, personenbezogene Daten von Kunden nicht auszudrucken oder lokal zu speichern, Arbeitsmaterialien grundsätzlich nicht unbeaufsichtigt liegen zu lassen und ordentlich zu verstauen. Unterlagen mit personenbezogenen Daten sind nach Gebrauch entweder in abschließbaren Schränken oder Schubfächern zu verstauen oder datenschutzgerecht zu entsorgen.
Öffentliche drahtlose Netzwerke und Verbindung mit dem Firmennetz	Öffentliche drahtlose Netzwerke werden ausschließlich über eine VPN-Verbindung, welche von Acture bereitgestellt wird, verwendet. Acture stellt sicher, dass Dritte nicht auf Daten des Auftraggebers zugreifen oder diese zur Kenntnis nehmen können.
1.3. Zugriffskontrolle	
Rollen- und Berechtigungskonzept	**Rollen- und Berechtigungskonzept Kunden-System** Administratoren des Auftraggebers können ein mehrstufiges Rollenkonzept zur Rechtevergabe individuell konfigurieren und dabei innerhalb der Software des Auftragnehmers zwischen Benachrichtigungs-, Ansichts-, und Bearbeitungsrechten je Funktion bzw. Thema für individuelle Nutzer unterscheiden. **Rollen- und Berechtigungskonzept Admin-System** Der Zugriff auf das Admin-System ist grundsätzlich auf geschulte Beschäftigte von Acture im Bereich Vertrieb, Kundenservice und Produktentwicklung beschränkt. **Rollen- und Berechtigungskonzept Server-/Datenbank-System**

	Der Zugriff auf das Server-/Datenbank-System ist grundsätzlich auf eine begrenzte Anzahl geschulter Beschäftigter im Bereich Produktentwicklung und Infrastruktur beschränkt.
Kontrolle der Zugriffsberechtigung für Acture auf Kunden-Systeme durch Auftraggeber	Der Auftraggeber kann Acture berechtigen, Zugriff auf das Kunden-System zu nehmen. Hierzu informiert der Auftraggeber den Auftragnehmer grundsätzlich in Textform. Mündliche Weisungen sind nur in Eilfällen gestattet und durch den Auftraggeber unverzüglich schriftlich oder in einem hierfür von Acture angebotenen elektronischen Format zu bestätigen.
Vergabe von Zugriffsrechten	Die Vergabe von Zugriffsrechten erfolgt bei Acture grundsätzlich nach dem „Need-to-Know“-Prinzip. Zugänge erhalten demnach ausschließlich Beschäftigte, die ihn nachvollziehbar und für die notwendige Dauer benötigen. Das Berechtigungskonzept ist rollenbasiert. Jedem Beschäftigten wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein. Die Zugriffsberechtigungen werden zentral dokumentiert sowie unmittelbar nach Erlöschen der Notwendigkeit des Zugriffs vom Administrator entzogen. Die Zugänge werden auf die minimal notwendigen Privilegien beschränkt. Zugriffe auf Admin-System oder Server-/Datenbank-System werden durch das Management, die Leitung der Infrastruktur-Abteilung oder den Information Security Manager freigegeben und erfolgen in der Regel nach dem 4-Augen-Prinzip. Die Administratoren bzw. der Information Security Manager prüfen regelmäßig, ob erteilte Berechtigungen noch erforderlich sind. Vorgesetzte sind darüber hinaus verpflichtet, im Falle eines Aufgabenwechsels von Beschäftigten eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen. Im Falle des Ausscheidens von Beschäftigten informieren die Personalverantwortlichen die Administratoren bzw. die Personalabteilung unverzüglich über anstehende Veränderungen, damit die entsprechenden Berechtigungen entzogen werden können. Der Entzug von Berechtigungen hat nach Möglichkeit binnen 24 Stunden nach Ausscheiden eines Beschäftigten zu erfolgen.
Host-basiertes Angriffserkennungssystem (HIDS)	Jedes Server-System ist mit einem Host-basierten Angriffserkennungssystem ausgestattet. Dieses überwacht mindestens Parameter wie auffällige System-Log-Einträge, Signaturen bekannter Rootkits und Trojaner, Auffälligkeiten im Device File System oder Brute Force-Angriffe. Alle Parameter mit Ausnahme der Änderungen an Dateisystemen werden in Echtzeit ausgewertet. Dateisysteme werden mindestens einmal täglich überprüft. Im Falle von Auffälligkeiten werden die zuständigen Mitarbeiter (Betrieb und Produktentwicklung) sofort mittels E-Mail-Benachrichtigung informiert.
Einsatz einer Paketfilter-Firewall	Die Server von Acture nutzen Paketfilter-Firewalls, die sicherstellen, dass keine Dienste direkt aus dem Internet erreichbar sind. Öffentlich erreichbare Dienste werden über Loadbalancer oder Bastion-Hosts geleitet, die ausschließlich die Protokolle, die für den jeweiligen Dienst benötigt werden, zulassen.
Protokollierung von An- und Abmeldevorgängen	Anmeldeversuche zum und sowie Abmeldevorgänge vom Admin-, Kunden-System sowie Server-Systemen/-Software werden protokolliert (min. E-Mail-Adresse, Benutzer ID, Ergebnis des Anmeldeversuchs sowie Zeitstempel) und derzeit für bis zu 30 Tage aufbewahrt. Diese Protokolle können auf Anfrage und/oder bei konkretem Verdacht ausgewertet werden.
1.4. Trennungskontrolle	
Trennung von Entwicklungs-, Test- und Betriebsumgebungen	Daten aus der Betriebsumgebung dürfen nur in Test- oder Entwicklungsumgebungen überführt werden, wenn sie vor der Überführung vollständig anonymisiert wurden. Die Übertragung der anonymisierten Daten muss verschlüsselt oder über ein vertrauenswürdiges Netz erfolgen. Software, die in die Betriebsumgebung überführt werden soll, muss zuerst in einer identischen

	Test-Umgebung („Staging“) getestet werden. Programme für Fehleranalysen oder das Erstellen/Kompilieren von Software dürfen in der Betriebsumgebung nur verwendet werden, wenn sich dies nicht vermeiden lässt. Dies ist vor allem dann der Fall, wenn Fehlersituationen von Daten abhängig sind, die aufgrund der Anforderungen für die Anonymisierung bei der Überführung in Testumgebungen verfälscht würden.
Softwareseitige Mandantentrennung	Acture stellt die getrennte Verarbeitung und Speicherung von Daten unterschiedlicher Auftraggeber über eine logische Mandantentrennung auf Basis einer Multi-Tenancy-Architektur sicher. Die Zuordnung und Identifizierung der Daten erfolgt dabei über die Zuweisung einer eindeutigen Kennung je Auftraggeber (bspw. Kundennummer/ „Company ID“). Die Absicherung der Architektur erfolgt durch die Implementierung von Integrationstests, welche sicherstellen, dass keine Datenbank-Abfragen ohne Abfrage und Zuordnung zu dieser Kennung durchgeführt werden und das Risiko der Umgehung der Mandantentrennung durch Programmierfehler minimiert wird. Regelmäßige Security-Audits sowie verbindliche Code-Reviews (4-bis 6-Augen-Prinzip) sichern die Architektur zusätzlich ab.
1.5. Pseudonymisierung	
Schlüsselverwaltung	Zum Gebrauch, zum Schutz und zur Lebensdauer von Schlüsseln sowie zum Einsatz von Verschlüsselungsverfahren nach dem Stand der Technik setzt Acture eine Richtlinie zur Verwendung von kryptographischen Verfahren um. Demnach erfolgt die Generierung und Verwaltung des Hauptschlüssels („Master Key“) außerhalb der Infrastruktur des von Acture eingesetzten Rechenzentrumsbetreibers. Eine Übertragung der Schlüssel außerhalb der Virtual Private Cloud und die Speicherung innerhalb der genutzten Infrastruktur erfolgt ausschließlich verschlüsselt. Der Zugriff auf die Schlüsselverwaltung wird protokolliert und automatisiert sowie bei konkretem Verdacht durch autorisiertes Personal von Acture auf Unregelmäßigkeiten überprüft. Die entsprechenden Schlüssel werden in regelmäßigen Abständen rotiert und bisher verwendete Schlüssel unmittelbar invalidiert und entfernt. Zudem werden Schlüssel strikt nach Netzwerken bzw. Datenbanken getrennt (bspw. keine Überführung eines Schlüssels in ein anderes Netzwerk). Im Rahmen einer regelmäßigen Sicherheitsprüfung wird sichergestellt, dass die Maßnahmen zur Schlüsselrotation wirksam sind und alte Schlüssel ordnungsgemäß entfernt wurden.
Datenbank- und Speicher-Verschlüsselung	Auf allen von Acture eingesetzten Datenbanken wird eine Verschlüsselung „at Rest“ nach dem Stand der Technik eingesetzt, sodass die Daten aus der Datenbank nur nach ordnungsgemäßer Authentifizierung am jeweiligen Datenbank-System gelesen werden können. Die zur Speicherung von Dokumenten eingesetzten Speichermedien („Storage“) werden ebenfalls auf Dateisystemebene verschlüsselt. Backups der Datenbank-Systeme werden ausschließlich verschlüsselt aufbewahrt.
Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen („Data in Transit“)	Alle personenbezogenen Daten, die von der Software von Acture an einen Client oder an andere Plattformen über ein unsicheres oder öffentliches Netzwerk übertragen werden, werden ausschließlich verschlüsselt übertragen. Dies gilt insbesondere auch für Zugriffe auf das Kunden- und Admin-System. Acture gewährleistet die Verwendung einer Verschlüsselungsmethode nach dem Stand der Technik in Abhängigkeit des auf Auftraggeber-Seite kompatiblen Verschlüsselungsalgorithmus (derzeit HTTPS-Verbindungen bzw. Transport Layer Security (TLS), Stichwort „Abwärtskompatibilität”: der Auftraggeber ist dafür verantwortlich, mit dem Stand der Technik kompatible Endgeräte/Browser einzusetzen). Administrative Zugriffe auf Server-Systeme von Acture sowie die

	Übertragung von Backups erfolgen ausschließlich über verschlüsselte Verbindungen, bspw. Secure Shell (SSH) bzw. Virtual Private Network (VPN).
Verschlüsselung von mobilen Datenträgern	Mobile Datenträger, auf denen Daten von Acture genutzt oder verarbeitet werden, werden ausschließlich verschlüsselt verwendet. Dies gilt insbesondere bei der Verwendung von USB-Sticks, externen Festplatten oder Ähnlichem. Grundsätzlich ist der Einsatz von mobilen Datenträgern zur Speicherung von Kundendaten jedoch nicht gestattet.
Verschlüsselung von Datenträgern auf Laptops	Es sind ausschließlich Laptops von Apple im Einsatz, um Angriffsmöglichkeiten auf die Systeme zu reduzieren. Auf allen Laptops der Beschäftigten wird eine entsprechende Festplattenverschlüsselung nach dem Stand der Technik eingerichtet.
Verschlüsselter Austausch von Informationen und Dateien	Grundsätzlich erfolgt der Austausch von Informationen und Dateien zwischen Auftraggeber und Acture direkt verschlüsselt. Sofern personenbezogene Daten oder vertrauliche Informationen des Auftraggebers auf Server übertragen werden müssen, die nicht über TLS-verschlüsselte HTTPS-Uploads gesendet werden können, so werden diese mit Secure File Transfer Protocol (SFTP) oder einem anderen verschlüsselten Mechanismus nach dem Stand der Technik übertragen. Der Auftraggeber ist dafür verantwortlich, diesen sicheren Datentransport bei Bedarf einzufordern oder bereitzustellen.
E-Mail-Verschlüsselung	Grundsätzlich werden alle von Beschäftigten von Acture oder innerhalb der Software von Acture versandten E-Mails mit TLS verschlüsselt. Ausnahmen können vorliegen, wenn der empfangende Mailserver kein TLS unterstützt. Der Auftraggeber trägt dafür Sorge, dass entsprechende im Rahmen des Auftrages verwendete Mailserver TLS-Verschlüsselung unterstützen.
1.6. Organisationskontrolle	
Organisationsanweisungen	Die Ziele im Datenschutz und in der Informationssicherheit sind in einer Datenschutz- und Informationssicherheits-Richtlinie festgelegt und für alle Beschäftigte von Acture verbindlich. Darüber hinaus sind weitere Organisationsanweisungen implementiert, um den Beschäftigten konkrete Richtlinien im Rahmen der Verarbeitung von personenbezogenen Daten zu vermitteln (bspw. Richtlinie zur Heim- und Telearbeit oder Richtlinie zur Nutzung von IT, Internet und E-Mail).
Bestellung eines Datenschutzbeauftragten nach Art. 37 DSGVO	Ein Datenschutzbeauftragter bzw. eine Datenschutzbeauftragte wurde von der Geschäftsführung bestellt. Er bzw. sie wirkt auf die Einhaltung der Vorschriften zum Datenschutz hin und erfüllt die Aufgaben im Sinne von Art. 39 DSGVO. Dazu zählen unter anderem die Unterstützung beim Aufbau und der Weiterentwicklung eines Datenschutzmanagementsystems, bei der Verfassung, Weiterentwicklung und Kontrolle entsprechender Richtlinien sowie bei der Durchführung regelmäßiger Sensibilisierungsmaßnahmen.
Verpflichtung auf Vertraulichkeit und Datenschutz	Alle Beschäftigten werden bei Aushändigung ihres Arbeitsvertrages bzw. spätestens zu Beschäftigungsbeginn schriftlich auf Vertraulichkeit und Datenschutz sowie auf sonstige einschlägige Gesetze verpflichtet. Die Verpflichtung gilt über die Beschäftigungsdauer hinaus. Freiberufliche Beschäftigte oder externe Dienstleister werden schriftlich anhand von Non-Disclosure-Agreements (NDAs) zur Verschwiegenheit verpflichtet und unterzeichnen zusätzlich einen Vertrag zur Auftragsverarbeitung, sofern durch sie personenbezogene Daten im Auftrag von Acture verarbeitet werden.
Datenschutzschulungen	Beschäftigte von Acture erhalten mit dem Arbeitsvertrag Informationen und Merkblätter zum Datenschutz und bestätigt deren Kenntnisnahme. Zusätzlich werden regelmäßige Schulungen (primär durch den Datenschutzbeauftragten) als Sensibilisierungsmaßnahmen durchgeführt. Mitarbeiter aus besonders sensiblen Bereichen wie bspw. Personalabteilung, Produktentwicklung oder Kundenservice

	erhalten bei Bedarf zudem gesondert Informationen und Schulungen zu spezifischen Fachthemen.
Einschränkung der Privat- und betrieblichen Nutzung von Kommunikationsmitteln	Es ist Beschäftigten von Acture nicht gestattet, das betriebliche E-Mail-System zur Privatnutzung zu verwenden. Das Internetsystem und die Telefondienste dürfen nur eingeschränkt privat genutzt werden. Es ist dabei strikt auf eine Trennung von privaten und betrieblichen Daten zu achten. Weiterhin ist es den Beschäftigten von Acture nicht gestattet, personenbezogene Daten oder sonstige Daten des Auftraggebers, insbesondere aus dem Auftrag, auf privaten Kommunikationsmitteln zu verarbeiten. Beschäftigte von Acture verpflichten sich zur Einhaltung entsprechender Richtlinien, deren Einhaltung im Rahmen des zulässigen und notwendigen Umfangs kontrolliert wird.
Personalsicherheit	Acture setzt Maßnahmen vor, während und nach der Beschäftigung zur Sicherstellung der Personalsicherheit um. Darunter fallen in der Regel: - Überprüfung und Bestätigung angegebener akademischer und beruflicher Qualifikationen - Vertragliche Vereinbarungen zur Festlegung von Verantwortlichkeiten und Verhaltensregeln - Durchführung von Schulungs-, Sensibilisierungs- sowie Kontrollmaßnahmen - Sensibilisierungs- und Sanktionsprozess bei datenschutzrechtlichen Verstößen - Durchführung eines dokumentierten Offboarding-Prozesses (inkl. Rücknahme von Schlüsseln, Entziehung von Zugriffsrechten, Sicherstellung der ausreichenden Dokumentation, Herausgabe und Weitergabe von Daten, Informationen und Wissen etc.) bei Beendigung des Arbeitsverhältnisses
2. Integrität	
2.1. Weitergabekontrolle	
Datenbank- und Speicher-Verschlüsselung ("Data at Rest")	Siehe Ziff. 1.5 "Pseudonymisierung".
Verbot der Weitergabe an unberechtigte Dritte	Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang der Weisungen und soweit dies zur Erbringung der vertraglichen Leistungen für den Auftraggeber erforderlich ist, erfolgen. Insbesondere ist eine Weitergabe von personenbezogenen Daten aus dem Auftrag an unberechtigte Dritte, bspw. durch Speicherung in einem anderen Cloud-Speicher, nicht zulässig.
Protokollierung der Weitergabe von Daten	Siehe Ziff. 2.2 "Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung".
2.2. Eingabekontrolle	
Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung	Wesentliche Systemaktivitäten werden protokolliert (mind. Benutzer ID, Rechte gemäß Rollenkonzept, Systemkomponenten oder Ressourcen, Art der durchgeführten Aktivitäten sowie Zeitstempel). Dazu zählen insbesondere die Eingabe, Änderung und Löschung von Daten, Nutzern und Berechtigungen sowie die Änderung von Systemeinstellungen. Auf Anfrage und/oder bei konkretem Verdacht kann eine entsprechende Auswertung der Protokolle durchgeführt werden.
3. Verfügbarkeit und Belastbarkeit	
3.1. Verfügbarkeitskontrolle	

Datensicherungsverfahren/ Backups	**Datensicherungsverfahren** Acture setzt zur Gewährleistung einer angemessenen Verfügbarkeit ein Backup-Konzept für die Datenbank mit den darauf gespeicherten Daten des Auftraggebers sowie für das Speichermedium mit entsprechenden gespeicherten Dokumenten nach dem Stand der Technik um. Backups werden täglich durchgeführt und 14 Tage in einem vom normalen Betrieb getrennten Speicher gesichert. Nach Ablauf der jeweiligen Fristen werden sämtliche Daten unwiederbringlich gelöscht. Es werden jeweils alle Dateien vollständig gesichert (nicht-inkrementell), sodass für das Wiederherstellen die Integrität von nur einem Backup gegeben sein muss. Das Ergebnis der Datensicherung wird vor der Übertragung in den Sicherungsspeicher mittels AES-Verschlüsselung mit einer Schlüssellänge von 256 bit verschlüsselt. Der Schlüssel wird in einem Schlüsselbund gesichert, auf den lediglich Administratoren Zugriff haben. Der vom normalen Betrieb getrennte Speicher wird mit denselben Vorkehrungen gesichert wie die Infrastruktur des normalen Betriebs: - Selektive Zugriffe nur für notwendige Personen (Administratoren) und Zwei-Faktor-Authentifizierung. - Erst bei einer Wiederherstellung der Daten wird die Sicherung außerhalb des Sicherungsspeichers wieder entschlüsselt. **Speicherbegrenzung** Um der Speicherbegrenzung gerecht zu werden, werden vor Inbetriebnahme einer wiederhergestellten Datensicherung die für personenbezogene Daten relevanten automatisierten Sperr- und Löschregeln auf die Daten angewandt. Hierdurch wird sichergestellt, dass Daten, welche zwischenzeitlich gelöscht wurden, aber in der Sicherung noch vorhanden waren, erneut gelöscht werden. Das Programm, welches die Daten sichert, wird ebenfalls zur Wiederherstellung der Daten genutzt. Sowohl Sicherung als auch Wiederherstellung werden dokumentiert und sind durch autorisierte Personen einfach umsetzbar.
Geo-Redundanz in Bezug auf Server-Infrastruktur der Produktiv-Daten und Backups	Zur Sicherstellung der Geo-Redundanz im Falle eines unvorhergesehenen Ereignisses, beispielsweise einer Naturkatastrophe, stellt Acture sicher, dass entsprechende Vorgaben der räumlichen Trennung in Bezug auf die Server-Infrastruktur der Produktiv-Daten und Backups gewährleistet ist. Dies kann durch die Verwendung unterschiedlicher Rechenzentren in ausreichender Entfernung oder von Rechenzentren unterschiedlicher Verfügbarkeitszonen sichergestellt werden.
Kapazitätsmanagement	Es existiert ein Kapazitätsmanagement inkl. Überwachung und automatischer Benachrichtigung der zuständigen Beschäftigten von Acture bei Kapazitätsengpässen.
Warnsysteme zur Überwachung der Erreichbarkeit und des Zustandes der Server-Systeme	Es existiert ein Warnsystem zur Überwachung der Erreichbarkeit und des Zustandes der Server-Systeme. Bei Ausfällen wird die Infrastruktur-Abteilung automatisch benachrichtigt, um unmittelbar Maßnahmen zur Problembeseitigung zu ergreifen.
IT-Störungsmanagement („Incident Response Management“)	Es existieren ein Konzept und dokumentierte Verfahren zum Umgang mit Störungen und sicherheitsrelevanten Ereignissen („Incidents“). Dies umfasst insbesondere die Planung und Vorbereitung der Reaktion auf Vorfälle, Verfahren zur Überwachung, Erkennung und Analyse von sicherheitsrelevanten Ereignissen sowie - im Rahmen der gesetzlichen Vorgaben - die Festlegung entsprechender Verantwortlichkeiten und Meldewege im Falle einer Verletzung des Schutzes personenbezogener Daten.

Weitere Maßnahmen zur Gewährleistung der Verfügbarkeit in den Rechenzentren	Im Rechenzentrum ist eine automatische Branderkennung und -bekämpfung installiert. Das System zur Branderkennung setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein. Alle Stromversorgungssysteme sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Das Rechenzentrum verfügt darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können. Das Rechenzentrum verfügt über eine Klimatisierung und Temperaturkontrolle. Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.
3.2. Wiederherstellbarkeit	
Regelmäßige Tests der Datenwiederherstellung („Restore-Tests“)	Es werden regelmäßige vollständige Restore-Tests zur Sicherstellung der Wiederherstellbarkeit im Falle eines Notfalls/einer Katastrophe durchgeführt.
Notfallplan („Disaster Recovery Concept“)	Es existiert ein Konzept zur Behandlung von Notfällen/Katastrophen sowie ein entsprechender Notfallplan. Acture stellt die Wiederherstellung aller Systeme auf Basis der Datensicherungen/Backups, in der Regel innerhalb von 24 Stunden, sicher.
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	
4.1. Datenschutzmaßnahmen	
Datenschutz- und Informationssicherheits-Team	Es ist ein Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
Risikomanagement	Es existiert ein Prozess zur Analyse, Bewertung und Zuordnung von Risiken, zur Ableitung von Maßnahmen auf Basis dieser Risiken sowie einer regelmäßigen Bewertung der Wirksamkeit dieser Maßnahmen im Rahmen des Datenschutz- und Informationssicherheits-Managementsystems von Acture.
Unabhängige Überprüfung der Informationssicherheit	**Durchführung von Audits** Es werden regelmäßig interne Audits zum Datenschutz und zur Informationssicherheit unter Gewährleistung der Unabhängigkeit des Prüfers (bspw. aus einem anderen Bereich oder extern) durchgeführt. Audits erfolgen dabei anhand gängiger Prüfkriterien/-schemata (insbesondere gesetzliche Vorgaben der DSGVO, Sicherheitsstandards etc.) und kontrollieren dabei insbesondere die Vollständigkeit und Richtigkeit von Richtlinien und Konzepten sowie die Dokumentation und Einhaltung entsprechender Prozesse. **Überprüfung der Einhaltung von Sicherheitsrichtlinien und -standards** Die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und sonstigen Sicherheitsanforderungen bei der Verarbeitung von personenbezogenen Daten wird regelmäßig überprüft. Diese Überprüfungen erfolgen nach Möglichkeit stichprobenartig und unvermutet. **Überprüfung der Einhaltung von technischen Vorgaben** Zur Überprüfung der Sicherheit der Anwendungen und Infrastruktur sowie der regelmäßigen Weiterentwicklung des Produkts werden regelmäßige automatisierte und manuelle Schwachstellenscans durch den Information Security Manager oder anderes qualifiziertes Personal durchgeführt. Es werden jährliche, detaillierte Penetrationstests durch einen externen Dienstleister

	durchgeführt, um die Anwendungen und Infrastruktur gezielt auf Schwachstellen zu untersuchen. **Prozess zur kontinuierlichen Verbesserung des Datenschutz- und Informationssicherheitsmanagementsystems** Die Prozesse zum Datenschutz und der Informationssicherheit beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Acture gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.
Auftragskontrolle	**Verarbeitung auf Weisung** Beschäftigte von Acture sind dazu angewiesen, personenbezogene Daten des Auftraggebers aus dem Auftrag ausschließlich auf dokumentierte Weisung im Rahmen des Auftragsverarbeitungsvertrages und der Nutzungsvereinbarung zu verarbeiten. Gemäß Auftragsverarbeitungsvertrag nimmt Acture Weisungen des Auftraggebers in schriftlicher Form sowie über die hierfür von Acture angebotenen elektronischen Formate entgegen. Mündliche Weisungen sind nur in Eilfällen gestattet und durch den Auftraggeber unverzüglich schriftlich oder in einem hierfür von Acture angebotenen elektronischen Format zu bestätigen. **Sorgfältige Lieferantenauswahl** Die Beauftragung von Lieferanten/Drittanbietern erfolgt bei Auslagerungen auf Basis eines sorgfältigen Auswahlprozesses in Zusammenarbeit mit dem Information Security Manager, dem Datenschutzbeauftragten und der Rechtsabteilung nach festgelegten Kriterien, insbesondere hinsichtlich des Datenschutzes und der IT-Sicherheit, dabei insbesondere: - Prüfung der Dokumentation und Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO - Je nach Schutzniveau und Umfang der personenbezogenen Daten, soweit möglich, Beauftragung von nur ISO/IEC 27001 zertifizierten Unternehmen (gilt in jedem Fall für Rechenzentren) Zur Risikoprävention wird im Rahmen des Prozesses ebenfalls eine Risikobewertung für die jeweiligen Lieferanten durchgeführt, sofern diese regelmäßig mit personenbezogenen Daten arbeiten. **Auftragsverarbeitung gemäß Art. 28 DSGVO** Eine Beauftragung und Nutzung eines Unterauftragnehmers erfolgt ausschließlich im Einklang mit dem Auftragsverarbeitungsvertrag zwischen Acture und dem Auftraggeber und mit den gesetzlichen Bestimmungen, sowie nach Abschluss einer entsprechenden Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen Acture und dem Unterauftragnehmer. Diese Vereinbarung hat nach Möglichkeit regelmäßig mindestens folgende Aspekte zu berücksichtigen: - Vereinbarung wirksamer Kontrollrechte (im Einklang mit Rechten des Auftraggebers, nach Möglichkeit auch Vor-Ort-Kontrollen) - Vereinbarung entsprechender Kontroll- und Auskunftsrechte bei der Beauftragung weiterer Unterauftragnehmer - Vereinbarung von Vertragsstrafen bei Verstößen, sofern notwendig und möglich - Ausschließliche Verarbeitung auf dokumentierte Weisung - Ausschluss unzulässiger Verarbeitungsschritte

	- Verbot der Anfertigung von Kopien von personenbezogenen Daten (ausgenommen Sicherungskopien/Backups) - Verpflichtung der Mitarbeiter des Unterauftragnehmers auf Vertraulichkeit - Mitwirkung bei der Wahrung der Betroffenenrechte - Bestellung eines Datenschutzbeauftragten, sofern gesetzlich vorgeschrieben - Informationspflichten bei meldepflichtigen Verletzungen des Schutzes personenbezogener Daten nach den Art. 33 und 34 DSGVO, Betriebsstörungen sowie sonstigen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten - Sicherstellung der Löschung/Vernichtung von Daten nach Beendigung des Auftrags Durchführung regelmäßiger Kontrollen/Einforderung von Nachweisen Acture wird sich vor Beginn der Beauftragung und danach regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen der von ihr eingesetzten Unterauftragnehmer überzeugen bzw. diese nachweisen lassen.
4.2. Incident-Response-Management	
Firewall und Spamfilter	Acture stellt sicher, dass Firewalls, Spamfilter und ähnliche Technologien gemäß den Best Practices der Branche konfiguriert sind und regelmäßig aktualisiert werden.
Security-Incident-Event-Management-System	Acture verwendet ein Security-Incident-Event-Management-System, um umfassende Protokolle von wichtigen Netzwerkgeräten und Hostsystemen zu erfassen.
Dokumentation von Sicherheitsvorfällen und Datenpannen	Bei einem Sicherheitsalarm werden Vorfälle an den Information Security Manager eskaliert. Der Information Security Manager ist in der Reaktion auf Sicherheitsvorfälle geschult und mit den jeweiligen Kommunikationskanälen und Eskalationspfaden vertraut.
4.3. Datenschutzfreundliche Voreinstellungen	
Minimalprinzip	Acture erhebt nicht mehr personenbezogene Daten, als für den jeweiligen Zweck erforderlich sind. Alle nicht zwingend für die Funktion der Anwendung notwendigen Angaben sind freiwillig. Für Nutzer der Software Acture besteht stets die Möglichkeit, Anliegen anonym anzugeben.
Need-to-Know Prinzip	Die Zugriffsrechte sind automatisch an die verschiedenen Benutzerrollen angepasst bzw. beschränkt. Die Zugriffsrechte der Beschäftigten von Acture auf Endgeräte, die an das Netzwerk von Acture angeschlossen sind, sind automatisch beschränkt.