Anlage

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO / Datenbearbeitung nach Art. 8 DSG

Stand: 27.09.2023

Der Anbieter erbringt für den Kunden Leistungen Unified Endpoint Management, welche im Hauptvertrag im Einzelnen beschrieben und durch dessen Vertragsanlagen definiert sind. Soweit der Anbieter dabei personenbezogen Daten / Personendaten im Auftrag und nach Weisung des Kunden verarbeitet schließen die Parteien nachfolgende Vereinbarung als Anlage zum Hauptvertrag. Der Anbieter ist nachstehend als Auftragsverarbeiter / Auftragsbearbeiter genannt. Der Kunde Auftraggeber. Soweit hierin keine Regelungen getroffen werden gelten die Bestimmungen des Hauptvertrags.

1. Allgemeines

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Unified Endpoint Management-Plattform. Hierzu gehören u.a. Lösungen für Mobile Device, Mobile App und Mobile Content Management, Digital Signage Management, Gateway Lösungen sowie IoT-Management. Die Einzelheiten sind im zugrundeliegenden Auftrag und in Ziff. 3 beschrieben.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutzgrundverordnung, kurz DSGVO. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag.

(3) Dieser Vertrag erfüllt sogleich die Anforderungen von Art. 9 (Datenbearbeitung durch Auftragsbearbeiter) des Schweizerischen Bundesgesetz über den Datenschutz (DSG).

(4) Anlage 2 dieser Vereinbarung erfüllt zugleich die gesetzlichen Anforderungen nach Schweizer Recht, namentlich nach Art. 8 DSG und Art. 3 DSV (Datenschutzverordnung).

(5) Soweit nicht abweichend geregelt meint personenbezogene Daten nach DSGVO auch Personendaten nach DSG:

2. Auslegung, Vorrang

(1) Werden hierin die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

(2) Im Falle eines Widerspruchs zwischen diesen Bestimmungen und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Bestimmungen Vorrang.

3. Gegenstand und Dauer des Auftrags

(1) Gegenstand der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst alle Tätigkeiten, die der Auftragnehmer gemäß den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen mit dem Auftraggeber erbringt und die eine Auftragsverarbeitung darstellen. Der Gegenstand des Auftrags im Einzelnen ergibt sich aus der Leistungsvereinbarung gem. **Anlage 1** (Beschreibung der Dienstleistungen) und der zugrundeliegenden Beauftragung. Dies gilt auch, sofern die Leistungsbeschreibungen und die jeweiligen vertraglichen Vereinbarungen nicht ausdrücklich Bezug nehmen auf diese Vereinbarung zur Auftragsverarbeitung.

(2) Dauer der Verarbeitung

Die Verarbeitung erfolgt zeitlich unbefristet, sofern dies in den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen nicht anders vereinbart ist. Eine Kündigung der Auftragsvereinbarung ist frühestens zum Ende der Leistungsvereinbarung (Hauptvertrag) mit einer Frist von 3 (drei) Monaten möglich. Mit Kündigung des Hauptvertrags endet automatisch diese Auftragsvereinbarung. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt hiervon unberührt.

4. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten: Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO. Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung gem. Anlage 1 (Beschreibung der Dienstleistungen).

(2) Arten der personenbezogenen Daten sind alle Arten personenbezogener Daten, die Auftragnehmer im Auftrag des Auftraggebers verarbeitet. Hiervon umfasst sind auch besondere Kategorien personenbezogener Daten. Gegenstand der Verarbeitung

personenbezogener Daten sind insbesondere folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien). Die Einzelheiten sind in Anlage 1 beschrieben.

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen sind in Anlage 1 beschrieben.

(4) Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in der Schweiz oder einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Ziff. 9 bleibt unberührt.

5. Pflichten der Parteien

5.1 Weisungen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber verbindlich bestätigt oder geändert wird.

(4) Soweit vereinbart gilt: Nur die folgenden namentlich genannten Personen (oder deren Vertreter soweit vereinbart) sind für den Auftraggeber weisungsberechtigt: In Anlage 1 beschrieben. Sofern keine ausdrückliche Benennung hierin erfolgt, werden sich die Parteien bei Bedarf individualvertraglich hierüber verständigen.

5.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anlage 1 genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

5.3 Sicherheit der Verarbeitung

(1) Der Auftragsverarbeiter ergreift mindestens die in Anlage 2 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.4 Verpflichtung zur Vertraulichkeit und der Einhaltung der Anforderungen nach der DSGVO, fachliche Eignung

(1) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen auf die Einhaltung der Anforderungen nach der DSGVO verpflichtet wurden. Der Auftraggeber hat das Recht, sich auf Anfrage durch Einsicht in die Verpflichtungs-/Hinweiserklärungen vom Inhalt und Umfang der Verpflichtung zu überzeugen.

(2) Der Auftragnehmer wird nur fachlich geeignete Personen bei der Verarbeitung der personenbezo-

genen Daten einsetzen. Er gewährleistet regelmässige Schulungen und Unterweisungen in Fragen des Datenschutzes und der Informationssicherheit.

5.5 Dokumentation und Einhaltung der Bestimmungen

(1) Die Parteien müssen die Einhaltung der Bestimmungen nachweisen können.

(2) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Bestimmungen umgehend und in angemessener Weise.

(3) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Bestimmungen festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Bestimmungen fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

(4) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

(5) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung

(6) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(7) 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, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

6. Internationale Datenübermittlungen

(1) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

(2) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind. Art. 44 ff. DSGVO im Übrigen bleibt unbeührt.

7. Technisch-organisatorische Maßnahmen (TOM) / Datensicherheit nach Art. 8 DSG

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c), 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 Einzelheiten sind in Anlage 2 geregelt.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

8. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

(1) Der Auftragnehmer ist zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet. Der Auftragnehmer setzt bei der Durchführung der 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 verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(2) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO ist in Anlage 2 geregelt.

(3) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, 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 Person gewährleistet wird.

10. Einsatz von Unterauftragsverarbeitern

(1) Der Auftraggeber erteilt dem Auftragnehmer die grundsätzliche Genehmigung Unterauftragsverarbeiter in Anspruch zu nehmen. Zum Zeitpunkt der Vertragsunterzeichnung bestehen folgende Unterauftragsverarbeiter (Liste):

- Host Europe GmbH, Hansestrasse 111, 51149 Köln
- AppTec Services GmbH, Engelbergerstr. 21, D-79106 Freiburg

(2) Die Auslagerung auf weitere Unterauftragsverarbeiter oder der Wechsel bestehender Unterauftragsverarbeiter sind zulässig. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 4 Woche im Voraus über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(3) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Bestimmungen gelten.

(4) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt

(5) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen und Garantien nach Art. 44 ff. DSGVO sicher.

(6) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

11. Unterstützungspflichten des Auftragnehmers

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er

von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

(2) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Wahrung von Betroffenenrechten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen.

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden (vgl. Ziff. 13).

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

d) die Unterstützung des Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

e) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

12. Meldung der Verletzung des Schutzes personbezogener Daten

12.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679 die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

12.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

13. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind lediglich Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht die Auftragnehmerin nach Wahl des Kunden entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach deutschem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt.

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

(4) Der Auftragnehmer verzichtet auf die Geltendmachung von Zurückbehaltungsrechten im Sinne von § 273 BGB an den von ihm verarbeitenden personenbezogenen Daten.

14. Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung als ungültig erweisen, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die ungültige Bestimmung ist durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Ungültigkeit des jeweiligen Punktes gedacht. Soweit diese Vereinbarung eine unbewusste Regelungslücke enthält, ist diese durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Regelungsbedürftigkeit des jeweiligen Punktes gedacht.

15. Formerfordernis

Änderungen und Ergänzungen dieser Bedingungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – sind gemäß DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

16. Schlussbestimmungen

(1) Auf diese Auftragsverarbeitung und alle in diesem Zusammenhang erbrachten Verarbeitungstätigkeiten findet das Recht des Hauptvertrages Anwendung.

(2) Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung gleich aus welchem Rechtsgrund ist im Hauptvertrag vereinbart.

(3) Änderungen dieser Vereinbarung bedürfender Schriftform. Das gilt auch für die Aufhebung des Schriftformerfordernisses.

(4) Sollte Bestimmungen dieser Vereinbarung unwirksam sein oder werden bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. In diesem Fall ist die unwirksame Bestimmung durch die gesetzliche/n Regelung/en zu ersetzten

Die folgenden Anlagen sind integraler Bestandteil dieser Vereinbarung

Anlage 1 – Beschreibung der Services, Art der Daten, Kategorien der betroffenen Personen, Weisungsberechtigte Personen des Auftraggebers

Anlage 2 – Technisch-organisatorische Maßnahmen / Datensicherheit

Anlage 1 – Beschreibung der Services, Dauer der Verarbeitung, Art der Daten, Kategorien der betroffenen Personen, Weisungsberechtigte Personen des Auftraggebers

1. Beschreibung der Services (Art der Verarbeitung und Zwecke)

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Unified Endpoint Management-Plattform. Hierzu gehören u.a. Lösungen für Mobile Device, Mobile App und Mobile Content Management, Digital Signage Management, Gateway Lösungen sowie IoT-Management. Gegenstand der Auftragsdatenverarbeitung ist die Bereitstellung (Hosting) der AppTec Software & AddOns zur Nutzung durch den Auftraggeber im Wege des Zugriffs über das Internet. Die Einzelheiten sind im zugrundeliegenden Auftrag beschrieben.

2. Dauer der Verarbeitung: siehe Ziff. 3 der AV

3. Art der personenbezogenen Daten (bitte zutreffendes ankreuzen)

- ☒ **Personenstammdaten**
- ☒ **Kommunikationsdaten**
- ☒ **Login Daten**
- ☒ **Personenzugeordnete Gerätedaten**
- ☒ **Logfiles und Protokolldaten**
- ☒ **IP Adressen, Geolokalisationsdaten**
- ☒ **Browserverlauf, Favoriten**
- ☒ **E-Mail Kommunikation und Anhänge**
- ☒ **Nutzungsdaten, soweit nicht vorstehend erfasst**
- ☐ **Sonstige (bitte beschreiben)**

4. Kategorien der betroffenen Personen (bitte zutreffendes ankreuzen)

- ☒ **Mitarbeiter des Auftraggebers**
- ☒ **Kunden, Geschäftspartner und Dienstleister**
- ☒ **(Geschäfts)Kontakte des Auftraggebers**
- ☒ **Anfragende / Interessenten des Auftraggebers**
- ☒ **E-Mail (Sender und Empfänger)**
- ☒ **Telefonie (Anrufer und Angerufene)**
- ☒ **Alle sonstigen Personen, welche auf Systemen des Auftraggebers verarbeitet werden und deren personenbezogene Daten der Auftragnehmer im Auftrag im Rahmen der Leistungserbringung verarbeitet**

Anlage 2 – Technisch und organisatorische Maßnahmen nach Art. 32 DSGVO / Datensicherheit nach Art. 9 DSG / Art. 3 DSV

A. Pseudonymisierung Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Getroffene Maßnahmen:

- ☒ Einsatz von VPN
- ☒ Transportverschlüsselung bei Fernwartungszugriffen
- ☒ Verschlüsselung von Mobile Device (Smart Phone, Tablett)
- ☒ Festplattenverschlüsselung Laptop

B. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1. Zutrittskontrolle

Gewährleistung, dass der Zutritt zu den Geschäftsräumen nur berechtigten Personen möglich sind:

Getroffene Maßnahmen:

- ☒ Geschäftsräume des Auftraggebers können nur durch Haupteingänge betreten werden und sind durch elektronische Zutrittskontrollsysteme, Schlüsselsysteme, den Einsatz von Alarmanlagen und besondere bauliche Maßnahmen geschützt
- ☒ Besucheranmeldung, Begleitung von Besuchern
- ☒ Zutritt zu den Büroräumen haben nur die entsprechenden Mitarbeiter
- ☒ Schlüssel / Schlüsselvergabe: Eine Organisationsanweisung zur Ausgabe von Schlüsseln existiert. Die Verwaltung der Schlüssel verantwortet der Standortverantwortliche.
- ☒ Türsicherung (elektrische Türöffner usw.)
- ☒ Videoüberwachung

2. Zugangskontrolle

Gewährleistung, dass nur Mitarbeiter der verantwortlichen Stelle oder Arbeitskräfte, die im Rahmen einer Auftragsverarbeitung verpflichtet sind, in den hierfür vorgesehenen Aufgabenbereich dürfen und mit Benutzeridentifikation entsprechende Daten verarbeiten:

Getroffene Maßnahmen:

- ☒ Es existiert eine Passwort- und Benutzerverwaltung. Benutzerkonten sind personenbezogen.
- ☒ Ein vom System vorgegebener Änderungszyklus für Benutzerpasswörter ist an allen Computerarbeitsplätzen eingerichtet (Änderungszyklus)
- ☒ Wartungsarbeiten bedürfen unserer ausdrücklichen Zustimmung. Sie dürfen nur begonnen werden, wenn sich das Wartungspersonal mit Benutzerkennung und Passwort angemeldet hat.
- ☒ Zugänge zur Authentifizierung am System werden ausschließlich neu und personenbezogen generiert
- ☒ Digitale Zertifikate

3. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugriff haben:

Getroffene Maßnahmen:

- ☒ Bildschirmsperre
- ☒ Authentifikation mit Benutzer und Passwort
- ☒ Auftragnehmern werden nur die Zugriffsrechte eingeräumt, die diese zur Durchführung der Wartungsarbeiten tatsächlich benötigen
- ☒ Eine Reihe von Hardware- und Softwareidentifikationsmaßnahmen, die Verschlüsselung der Daten bei der Datenübertragung sowie ein mehrstufiges Zugriffs- und Nutzungskontrollverfahren schließen den unbefugten Zugriff auf die gespeicherten Datenbestände und die unberechtigte Kenntnisnahme aus
- ☒ Benutzerbezogene Protokollierung der (Fehl-)Anmeldung
- ☒ Es wird sichergestellt, dass IT-Personal nur insoweit auf gespeicherte personenbezogene Daten zugreifen kann, als dies zur Durchführung von Wartungsarbeiten unerlässlich notwendig ist
- ☒ Ein Berechtigungskonzept gewährleistet, dass personenbezogene und andere schutzwürdige Daten gegen zufällige Zerstörung oder Verlust geschützt sind
- ☒ Einsatz von Aktenvernichtung
- ☒ Ordnungsgemäße Vernichtung und/oder Löschung von Datenträgern (DIN 66398)

4. Benutzerkontrolle

Gewährleistung der Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

Getroffene Maßnahmen:

- ☒ Einsatz Berechtigungskonzept
- ☒ Gruppenberechtigungen sind flach und übersichtlich aufgebaut und werden nicht kaskadiert verwendet
- ☒ Definierte Rechteprofile für die verschiedenen Funktionsbereiche werden explizit zugeteilt und dabei zentral administriert

5. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Die Plausibilisierung der Dateneingabe findet dabei auf revisionsrelevanten Feldern statt und wird entsprechend der zugehörigen Prozesse validiert.

Getroffene Maßnahmen:

- ☒ Protokollierung der Systemnutzung und Auswertung der Protokollierung
- ☒ Ein mehrstufiges Protokollverfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können

6. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung; das heißt, alle in die Datenverarbeitung eingebundenen Abteilungen sind funktionell, organisatorisch getrennt. Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zu Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist.

Getroffene Maßnahmen:

- ☒ Die Trennung erfolgt über die Zugriffsregelungen
- ☒ Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zu Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist
- ☒ In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung
- ☒ Trennung von Produktiv- und Testsystemen sowie Ordnerstrukturen und Datenbanken

C. Integrität (Art. 32 Abs. 1 lit. c) DSGVO)

7. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können:

Getroffene Maßnahmen:

- ☒ Softwareseitiger Ausschluss (Mandantentrennung, Datei-Separierung)
- ☒ Einsatz eines zentralen Patchmanagements für Softwarekomponenten

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Getroffene Maßnahmen:

- ☒ Daten werden nur in verschlüsselter Form übermittelt (Transportverschlüsselung bei Fernwartungszugriffen)
- ☒ Es existieren Richtlinien und Verfahrensanweisungen, in welchen die Nutzung sowie der korrekte Umgang mit mobilen Datenträgern, Geräten und Kommunikationsmitteln vorgegeben werden. Ebenso eine Richtlinie zum Umgang mit fehlerhaften Druckerzeugnissen.
- ☒ Strenge Richtlinien und Arbeitsanweisungen beim Auftragnehmer gewährleisten, dass eine unbefugte Weitergabe oder das Entfernen von Daten verhindert wird
- ☒ Entsorgungsgut mit schutzwürdigem Inhalt wird unter Beachtung der Sicherheitsstufen des Grad der Vernichtung nach DIN 66399 vernichtet

9. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Getroffene Maßnahmen:

- ☒ Protokollierung der Datenübermittlungsstelle/-wege, welche im Verdachtsfall ausgewertet werden können
- ☒ Die technische Absicherung erfolgt über Firewall und Proxysysteme
- ☒ Soweit technisch möglich und wirtschaftlich vertretbar, werden geeignete Verschlüsselungstechnologien eingesetzt (siehe Transportverschlüsselung bei Fernwartung)

10. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind:

Alle anfallenden personenbezogenen Daten werden nur entsprechend den jeweils geltenden Vorschriften zum Schutz personenbezogener Daten, nur zum Zwecke der jeweiligen Auftragsabwicklung sowie zur Wahrung berechtigter eigener Geschäftsinteressen im Hinblick auf die Beratung und Betreuung von Kunden und zur Abwicklung der arbeitsvertraglichen Grundlagen verarbeitet.

Getroffene Maßnahmen:

- ☒ Protokollierung der Systemnutzung und Auswertung der Protokollierung
- ☒ Ein mehrstufiges Protokollverfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können
- ☒ Durchführung von Schulungsmaßnahmen für die Softwarenutzung
- ☒ Alle Mitarbeiter werden in regelmäßigen Abständen zum Datenschutz geschult
- ☒ Stichprobenprüfung der Datenverarbeitung

11. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Getroffene Maßnahmen:

- ☒ Ereignisprotokollierung der Systeme mit Meldung von Störungen
- ☒ Wartungsverträge und SLA-Vereinbarungen

12. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Getroffene Maßnahmen:

- ☒ Alle Dienstleister, welche die Möglichkeit haben, personenbezogene Daten einzusehen, werden gemäß Bundesdatenschutzgesetz auf das Datengeheimnis und zur Zweckbindung bei einer Auftragsverarbeitung verpflichtet
- ☒ Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben, Ausnahmen vom konkreten Weisungsrahmen gelten nur für technisch bedingte Verarbeitungen, z. B. zur internen Sicherung
- ☒ Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag unter Berücksichtigung der Pflichtinhalte sowie ferner durch die Anwendungsbeschreibung der Dienstleistung eindeutig vorgegeben
- ☒ Vereinbarungen nach Art. 28 DSGVO mit Auftragsverarbeitern
- ☒ Intercompany Vereinbarungen nach Art. 28 DSGVO mit verbundenen Unternehmen, weche Daten im Auftrag verarbeiten
- ☒ Standardvertragsklauseln (SCC) bei Übermittlung von Daten in Drittändern
- ☒ Auftragsbezogene Auskünfte werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt
- ☒ Umfassende vertraglich zugesicherte Kontrollrechte der Auftraggeber

D. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. c) DSGVO)

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

Ein mehrstufiges Protokollverfahren gewährleistet soweit möglich, dass keine Datenveränderungen unbemerkt vorgenommen werden können. Protokoliert wird sowohl auf Client als auch serverseitig. Schwerpunkt der Protokollierung liegt dabei auf Anwendungs-, System- und Sicherheitsebene.

Getroffene Maßnahmen:

☒ Es existieren Richtlinien und Verfahrensanweisungen für den sicheren Betrieb der IT-Umgebung. Ebenso existieren Virenschutz-, Datensicherungs- und Archivierungsmassnahmen.

14. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:

Zahlreiche Datensicherungsmaßnahmen gewährleisten, dass personenbezogene und andere schutzwürdige Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Getroffene Maßnahmen:

☒ Es bestehen Notfall- und Wiederherstellungspläne. Sicherungen werden nach einem definierten Backup-Plan täglich und wöchentlich durchgeführt.

☒ Einsatz von Raid-Systemen sowie Spiegelung der Datenbestände

☒ Mehrfache maschinelle und gegen unbefugten Zugriff gesicherte Auslagerung der Datensicherungsbestände

15. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern:

Getroffene Maßnahmen:

☒ Sicherheitsvorkehrungen gewährleisten, dass ein unbefugtes Entfernen von Datenträgern aus den Sicherheitsbereichen verhindert wird

☒ Inventarisierung aller Datenträger

E. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO)

Getroffene Maßnahmen:

- ☒ Regelmäsige Test der Applikationen
- ☒ Überprüfung der Maßnahmen im Rahmen der Wirksamkeitskontrolle des Informationssicherheitsmanagementsystems (ISMS – gemäß DIN ISO/IEC 27001)
- ☒ Kontinuierlicher Verbesserungsprozess im Rahmen ISMS
- ☒ Bestellung eines Datenschutzbeauftragten
- ☒ Den Datenschutzbeauftragten erreichen Sie wie folgt: datenschutzbeauftragter@apptec360.com
- ☒ Regelmäßige Datenschutz- / und IT-Sicherheits-Schulung der zugriffsberechtigten Mitarbeiter
- ☒ Regelmässige Überprüfung der Verarbeitungsverzeichnisse und der Technischen und organisatorischen Massnahmen sowie bei Bedarf
- ☒ Audits der Wirtschaftsprüfer
- ☒ Kunden- und Lieferantenaudits