VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG (ART. 28, 29 DSGVO) INSIGN 365

Stand 12.08.2021
Version 1.7

Auftraggeber:

Lizenznehmer des Onlinedienstes inSign 365

Auftragnehmer / Auftragsverarbeiter:

iS2 Intelligent Solution Services AG
Am Bäckeranger 2
85417 Marzling

Präambel

Dieser Auftragsverarbeitungs-Vertrag regelt die Verpflichtungen der Vertragsparteien im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag oder Unterauftrag. Dieser AV-Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Dienstleistungsvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer Beauftragte (Subunternehmer) personenbezogene Daten (»Daten«) des Auftraggebers oder von dessen Auftraggeber (Unterbeauftragung) verarbeiten. In diesem AV-Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU - Datenschutzgrundverordnung zu verstehen.

1. Gegenstand und Dauer des Auftrags

1.1 Der Auftrag umfasst Folgendes:

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Auftraggeber sind konkret beschrieben im Dokument "AGB_inSign_365.pdf".

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

1.2 Diese Vereinbarung beginnt und endet automatisch mit dem Hauptvertrag (Ziffer 1.1), sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Pflichten oder Kündigungsrechte ergeben.

1.3 Das Recht beider Parteien zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen

2.1 Der Auftrag erfasst alle Arten von Verarbeitungen im Sinne der DSGVO. Der Auftraggeber hat folgenden Zweck festgelegt zur Verarbeitung personenbezogener Daten nach Maßgabe dieser Vereinbarung:

"AGB_inSign_365.pdf", Elektronische Vertragsabschlüsse, insbesondere die Erfassung von elektronischen Unterschriften.

2.2 Art der Daten und Kategorien betroffener Personen

Der Auftragnehmer verarbeitet personenbezogene Daten aller Kategorien (auch nach Art. 9 DSGVO) des Auftraggebers und der Interessenten und Kunden des Auftragsgebers.

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu schützen.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gemäß Art. 32 DSGVO, die mit dem Stand zum Zeitpunkt des Vertragsschlusses definiert sind in der Anlage zu 3.2.

3.3 Der Auftraggeber informiert sich vor Abschluss der Vereinbarung zur Auftragsverarbeitung und anschließend in regelmäßigen Abständen über die technischen und organisatorischen Maßnahmen des Auftragnehmers anhand der vom Auftragnehmer bereitgestellten Informationen gemäß Ziffer

8 dieser Vereinbarung. Der Auftragnehmer trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3.4 Eine Änderung der getroffenen Sicherheitsmaßnahmen nach Vertragsschluss bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.5 Wenn der Auftraggeber nach Abschluss dieser Vereinbarung entscheidet, dass die bislang vorhandenen technischen und organisatorischen Maßnahmen des Auftragnehmers zum Schutz bestimmter personenbezogener Daten unter Berücksichtigung der Kriterien des Art. 32 Absatz (1) DSGVO nicht ausreichen, wird er dem Auftragnehmer die zusätzlich erforderlichen Maßnahmen benennen und mit dem Auftragnehmer eine Vereinbarung dazu treffen, wer welche Maßnahmen zu welchen Kosten veranlassen wird.

4. Ort der Verarbeitung

Der Auftragnehmer verarbeitet die vereinbarungsgegenständlichen Daten in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

Der Auftragnehmer ist nur dann befugt, die Daten in einen Staat außerhalb der Europäischen Union bzw. außerhalb des Europäischen Wirtschaftsraums (sogenanntes „Drittland") zu verlagern, sofern hierfür das in der Datenschutz-Grundverordnung festgelegte Schutzniveau für die vertragsgegenständlichen Daten gemäß den Art. 44 ff. DSGVO gewährleistet wird.

5. Weisungsbefugnis - Berichtigung, Einschränkung und Löschung von Daten; Anfragen von betroffenen Personen

5.1 Der Auftragnehmer darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern ausschließlich im Rahmen der getroffenen Vereinbarungen bzw. nur nach dokumentierter Weisung des Auftraggebers verarbeiten, berichtigen, löschen oder deren Verarbeitung einschränken. Die Weisungen des Auftraggebers müssen sich im Rahmen der geltenden Datenschutzgesetze, dieser Vereinbarung und Hauptvertrags (Ziffer 1.1) halten.

5.2 Soweit die Weisungen des Auftraggebers nicht bereits in einem bestehenden Hauptvertrag (Ziffer 1.1) enthalten sind, erteilt er seine Weisungen ausschließlich durch die u.g. Weisungsberechtigten an die dort genannten Weisungsempfänger.

5.3 Falls der Auftragnehmer durch eine gesetzliche Vorschrift zu einer bestimmten Verarbeitung verpflichtet ist, zu welcher es keine Weisung des Auftraggebers gibt, teilt er dies dem Auftraggeber mit, sofern das Gesetz die Mitteilung nicht verbietet.

5.4 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung könnte gegen Datenschutzvorschriften verstoßen.

5.5 Weisungsberechtigte Person für den Auftraggeber ist der Lizenznehmer.

Weisungsempfänger beim Auftragnehmer ist/sind:

Martin Hierhager, Mirko Röder

5.2 Wenn sich ein Betroffener an den Auftragnehmer wendet zur Geltendmachung seiner Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung, wird der Auftragnehmer dieses Ersuchen nicht selbst erfüllen, sondern unverzüglich an den Auftraggeber weiterleiten und dessen Weisungen abwarten. Wenn der Auftraggeber das Ersuchen der betroffenen Person nicht, nicht richtig oder nicht fristgerecht beantwortet, haftet der Auftragnehmer nicht und der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter frei und ersetzt ihm etwaige Schäden und Aufwendungen.

Dies gilt nicht, soweit die unterbliebene, fehlerhafte oder nicht fristgerechte Antwort des Auftraggebers an die betroffene Person auf einer unterlassenen, fehlerhaften oder verspäteten Information vom Auftragnehmer an den Auftraggeber beruht.

6. Verantwortungsbereich des Auftraggebers

6.1 Datenschutz-Compliance:

Der Auftraggeber ist allein dafür verantwortlich, alle Voraussetzungen dafür herzustellen und nachzuweisen, dass die Verarbeitung der dem Auftragnehmer offenbarten personenbezogenen Daten nach Maßgabe dieser Vereinbarung zulässig ist. Insbesondere hat der Auftraggeber sicherzustellen, dass seine Weisungen den Datenschutzgesetzen entsprechen. Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung und die Beschreibung der betroffenen Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.

6.2 Sind die Weisungen des Auftraggebers nicht vom Leistungsumfang des Hauptvertrags gemäß Ziffer 1.1 dieser Vereinbarung umfasst, werden diese als Anforderung des Auftraggebers zur Erweiterung bzw. Änderung des vereinbarten Leistungsumfangs behandelt. Der Auftragnehmer teilt dann innerhalb angemessener Frist mit, ob und unter welchen Kosten er die weiteren Weisungen ausführen wird.

7. Verantwortungsbereich des Auftragnehmers

7.1 Der Auftragnehmer setzt folgende Maßnahmen um:

a) Sofern der Auftragnehmer gemäß den Vorgaben dieses Vertrags Unterauftragnehmer außerhalb der Europäischen Union einsetzt, trägt er dafür Sorge, dass jeder Unterauftragnehmer einen Vertreter nach Art. 27 Absatz (1) DSGVO benennt.

b) Die Wahrung der Vertraulichkeit gemäß den Art. 28 Absatz (3) Satz 2 lit. b, 29, 32 Absatz (4) DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten Bestimmungen zum Datenschutz vertraut sind. 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.

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

d) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, 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 bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) 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.

f) 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.

g) Nachweis der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber auf dessen Anforderung und im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages und der Erledigung aller Pflichten gemäß Ziffer 6 dieses Vertrags.

h) Für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers gemäß Art. 30 Absatz (1) DSGVO ist ausschließlich der Auftraggeber oder, im Falle der Unterbeauftragung, dessen Auftraggeber verantwortlich; der Auftragnehmer unterstützt den Auftraggeber dabei auf Anforderung durch Bereitstellung von Informationen, soweit dies die Verarbeitung personenbezogener Daten nach dieser Vereinbarung betrifft.

7.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Unterstützung des Auftraggebers bei dessen technischen und organisatorischen Maßnahmen,

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht (oder, im Falle der Unterbeauftragung, der seines Auftraggebers) gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung (oder, im Falle der Unterbeauftragung, der seines Auftraggebers) und

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Nach der Meldung einer Verletzung personenbezogener Daten durch den Auftragnehmer an den Auftraggeber entscheidet der Auftraggeber oder, im Falle der Unterbeauftragung, dessen Auftraggeber in alleiniger Verantwortung, ob die Voraussetzungen für eine Meldung an Behörden bzw. betroffene Personen vorliegen und nimmt die Meldungen in alleiniger Verantwortung vor.

7.3 Beim Auftragnehmer ist als fachkundiger Datenschutzbeauftragter benannt und bei der zuständigen Aufsichtsbehörde gemeldet:

Sven Lenz
Datenschutzkanzlei Lenz GmbH & Co. KG
Bahnhofstraße 50, D-87435 Kempten
www.datenschutzkanzlei-lenz.de
Telefon: +49 831 930653-00
E-Mail: sl@datenschutzkanzlei-lenz.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Auf Anfrage des Auftraggebers ist der aktuelle Fachkundenachweis zur Verfügung zu stellen.

8. Unterauftragsverhältnisse

8.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, Unterauftragnehmer einzusetzen.

Der Auftragnehmer ist dabei verpflichtet, den Unterauftragnehmer

a) unter Berücksichtigung seiner technischen und organisatorischen Maßnahmen zum Datenschutz sorgfältig auszuwählen und

b) durch schriftlichen oder elektronischen Vertrag zu beauftragen und

c) in Bezug auf den Unterauftrag mindestens in demselben Umfang zur Erfüllung datenschutzrechtlicher Anforderungen zu verpflichten, wie dies in dieser Vereinbarung für den Auftragnehmer gilt.

d) Sofern eine Einbeziehung von Unterauftragnehmern in Drittländern erfolgen soll, stellt der Auftragnehmer sicher, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DSGVO gewährleistet ist, zum Beispiel durch Abschluss einer Vereinbarung gemäß den von der EU-Kommission genehmigten EU-Standardvertragsklauseln.

Der Unterauftragnehmer muss einen Vertreter in der EU bestellt haben.

8.2 Die Parteien stellen fest, dass die Voraussetzungen gemäß Ziffer 8.1 für die Unterauftragsverhältnisse vorliegen, die zum Zeitpunkt des Abschlusses dieser Vereinbarung bereits bestehen.

Bevor der Auftragnehmer an den erteilten Unteraufträgen Änderungen vornimmt in Bezug auf die Hinzuziehung oder Ersetzung weiterer Unterauftragnehmer, teilt er dies dem Auftraggeber schriftlich oder in elektronischem Format mit. Der Auftraggeber kann gegen diese Änderung innerhalb einer Frist von 4 Wochen aus wichtigem Grund schriftlich oder in elektronischem Format Einspruch beim Auftragnehmer erheben.

8.3 Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

9. Nachweismöglichkeiten; Inspektionen und behördliche Kontrollen

9.1 Der Auftragnehmer weist dem Auftraggeber auf dessen Anfrage die Einhaltung der in dieser Vereinbarung geregelten Pflichten mit geeigneten Mitteln nach, wobei dem Auftragnehmer das Wahlrecht zwischen mehreren geeigneten Mitteln zusteht. Geeignet sind zum Beispiel

- eine Darstellung der aktuell getroffenen technischen und organisatorischen Maßnahmen über die Punkte gemäß der Anlage zu Ziffer 3.2 dieser Vereinbarung,
- Selbstauskünfte oder Prozessbeschreibungen des Auftragnehmers,
- Nachweise zur Durchführung von Selbstaudits,
- unternehmensinterne Verhaltensregelungen einschließlich eines externen Nachweises über deren Einhaltung,
- Zertifikate oder Testate zum Datenschutz und/oder zur Informationssicherheit
- genehmigte Verhaltensregelungen gemäß Art. 40 DSGVO,
- Zertifikate gemäß Art. 42 DSGVO.

9.2.1 Inspektionen (Vor-Ort-Kontrollen) beim Auftragnehmer durch den Auftraggeber oder von diesem beauftragte Prüfer finden nur statt nach vorheriger Abstimmung und Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit sowie zu den üblichen Geschäftszeiten. Der Auftraggeber muss gewährleisten, dass der Betriebsablauf des Auftragnehmers nicht gestört wird. Die Inspektionen durch vom Auftraggeber beauftragte Prüfer kann der Auftragnehmer von der Unterzeichnung einer Verschwiegenheitserklärung durch diesen abhängig machen.

9.2.2 Der Auftraggeber trägt die Aufwendungen des Auftragnehmers, die diesem im Rahmen der Inspektion entstehen; dies gilt auch für etwaige Prüfungen, die eine Datenschutz- oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers beim Auftragnehmer vornimmt.

9.3 Der Auftragnehmer hat in jedem Fall das Recht, die Duldung von Kontrollen und die Erteilung von Informationen insoweit und dann zu verweigern, wenn die Kontrolle bzw. Informationserteilung ein Risiko darstellen würde für die Sicherheit der Datenverarbeitungsanlagen oder der darauf befindlichen Daten des Auftragnehmers oder Dritter (zum Beispiel anderer Auftraggeber des Auftragnehmers). Sofern der Auftragnehmer berechtigte Gründe für ein Sicherheitsrisiko vorweist, werden sich die Vertragsparteien entsprechend auf eine alternative Kontrollmöglichkeit einigen.

10. Löschung und Rückgabe von personenbezogenen Daten; Vertraulichkeit auch nach Vertragsende

10.1 Im Falle einer Verpflichtung zur Datenlöschung gewährleistet der Aufragnehmer eine datenschutzgerechte Löschung der vertragsgegenständlichen personenbezogenen Daten nach dem Stand der Technik.

10.2 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.

10.3 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

10.4 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.

10.5 Der Auftragnehmer ist verpflichtet, während und auch über das Ende des Vertrags hinaus die Vertraulichkeit aller vertragsgegenständlichen Informationen, Unterlagen und elektronischen Daten zu gewährleisten.

11. Vergütung

Sofern die Maßnahmen des Auftragnehmers gemäß dieser Vereinbarung nicht ausdrücklich von einem Hauptvertrag (siehe oben Ziffer 1.1) und der dort geregelten Vergütung erfasst sind, sind sie zu den aktuell geltenden Preisen des Auftragnehmers gesondert zu vergüten.

12. Haftung

Für die Haftung des Auftragnehmers gelten die Bedingungen des Hauptvertrags.

13. Schlussbestimmungen

13.1 Für diese Vereinbarung gilt deutsches Recht. Die Vertragsparteien haben diese Vereinbarung auf der Grundlage des Entwurfs der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) abgeschlossen.

13.2 Sollte eine Vertragsbestimmung unwirksam sein oder werden, so berührt dies die Gültigkeit des übrigen Vertragsinhalts nicht. Die Vertragsparteien werden sich bemühen, in einem solchen Fall eine in ihrem wirtschaftlichen Ergebnis dem jetzigen Sinn entsprechende Lösung zu finden. Dies gilt auch, wenn bei Durchführung des Vertrags eine ergänzungsbedürftige Lücke offenbar wird.

13.3 Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

13.4 Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist München, wenn der Auftraggeber Kaufmann, eine juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Der Auftragnehmer ist jedoch berechtigt, an jedem anderen gesetzlichen Gerichtsstand zu klagen.

Unterauftragnehmer

Der Auftraggeber stimmt der Beauftragung folgender Unterauftragnehmer durch den Auftragnehmer zu.

	Service Provider	Zweck	Art der verarbeiteten Daten
☒	1&1 IONOS SE Elgendorfer Str. 57 56410 Montabaur	Bereitstellung von Cloud-Rechenzentrumsdienstleistungen (insbesondere Netzwerk, Computing, Storage, Backup)	Hostname und IP-Adresse von Kundenservern. Es findet keine originäre Nutzung oder Verarbeitung von Kundendaten durch den Subunternehmer statt.
☒	CM.com Germany GmbH Dr. Eugen Schön Straße 35 97332 Volkach	Bereitstellung von SMS-Diensten	Alle Informationen, die für die SMS-Kommunikation benötigt werden.
☒	rapidmail GmbH Augustinerplatz 2 79098 Freiburg i.Br.	Bereitstellung von E-Mail-Diensten	Alle Informationen, die für die E-Mail-Kommunikation benötigt werden.
☒	die Bayerische IT GmbH Thomas-Dehler-Str. 25 81737 München	Bereitstellung von Cloud-Rechenzentrumsdienstleistungen zur Langzeitarchivierung von Dokumenten	Informationen, die für die verschlüsselte Verarbeitung von Dokumenten benötigt werden. Es findet keine originäre Nutzung oder Verarbeitung von Kundendaten durch den Subunternehmer statt.
☒	D-Trust GmbH Kommandantenstraße 18 10969 Berlin	Bereitstellung von Diensten für qualifizierte elektronische Signaturen (qeS) und zur Identifikation von qeS-Nutzern (nur wenn vom Auftraggeber als Option beauftragt)	Alle Informationen, die zum Erstellen von, und Signieren mit, qualifizierten Zertifikaten benötigt werden.

Anlage zu 3.2 der Vereinbarung zur Auftragsverarbeitung
Technische und organisatorische Maßnahmen des Auftragnehmers

Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar. Die jeweils für Ihren Anwendungsfall erforderlichen technischen-organisatorischen Maßnahmen eingesetzter Unterauftragnehmer sind in diesem Dokument nicht mit aufgenommen und werden gesondert zur Verfügung gestellt. Unterauftragnehmer werden nach Art. 28 DSGVO sorgfältig ausgewählt und laufend überprüft.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennen die Gesetze verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

(1)Vertraulichkeit

(2)Integrität

(3)Verfügbarkeit und Belastbarkeit

(4)Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(5)Pseudonymisierung und Verschlüsselung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren. Diese Maßnahmen stellen wir in der Folge vor, um unseren Informationspflichten aus Art. 32 Abs. 3 lit. C nachzukommen.

Organisatorisches

Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. B, 29, 32 Abs. 4 DSGVO verpflichtet. Die bei der Datenverarbeitung eingesetzten Systemadministratoren sind auf ihre Geheimhaltungspflichten gemäß §203 StGB verpflichtet.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden.

Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von iS2 betrieben werden:

Kontrollziel	Maßnahmen
VERTRAULICHKEIT	
1. Zutrittskontrolle Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	■ Elektronische Zutrittskontrolle zum Firmengebäude und den zentralen Datenverarbeitungsanlagen (Serverraum) ■ Elektronische Protokollierung aller Schließvorgänge (Schlüsselnummer und Zeitstempel) ■ Zentrale Vergabe und Dokumentation der Vergabe der Schließberechtigungen ■ Meldeverpflichtung und Sperre der Zutrittsberechtigung bei Verlust ■ Zugang zu Serverräumen nur für autorisiertes Personal nach ausdrücklicher Genehmigung durch die Geschäftsleitung ■ Autorisiertes Wachpersonal für Notfälle 24/7 verfügbar und zutrittsberechtigt ■ Aufenthalt von nicht autorisierten Personen in Sicherheitsbereichen nur unter Aufsicht ■ sorgfältige Auswahl des Reinigungspersonals ■ Aktive Netzwerkkomponenten außerhalb des Serverraums befinden sich nur in verschlossenen Sicherheitsschränken
2. Zugangskontrolle Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	■ Schutz aller Datenverarbeitungsanlagen mindestens durch die Kombination aus Benutzerkennung und Passwort ■ Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten ■ Mindestanforderungen an Passwortkomplexität durch Kennwortrichtlinie ■ Kennwort-Neueingaben von Benutzern werden automatisch mit bekannten, kompromittierten Kennwörtern abgeglichen. Eine Verwendung solcher Kennwörter wird verhindert. ■ Kennwörter müssen geändert werden, wenn der Verdacht auf Kompromittierung des Kennworts (z.B. durch Offenlegung, Hackerangriff, etc.) besteht. ■ Falscheingabe des Passworts wird elektronisch protokolliert und führt im Wiederholungsfall zu einer zeitlich begrenzten Deaktivierung des Benutzerkontos ■ Verschlüsselte Speicherung von Kennwörtern

	■ Datenverarbeitungsanlagen sperren die Benutzereingabe, sofern über einen bestimmten Zeitraum keine Interaktion erfolgt ■ Einsatz von Multi-Faktor-Authentifizierung (MFA) zur Absicherung sensibler Administratorkonten, soweit technisch realisierbar ■ Netzwerksegmentierung, Verwendung einer Demilitarisierten Zone (DMZ) ■ Zugangsbeschränkung für bestimmte IP-Adressbereiche ■ Externer Zugang nur über sichere Verbindungen (VPN oder TLS-Verschlüsselung) ■ Durchführung regelmäßiger Softwareupdates ■ Automatisierte Vulnerability Scans als Teil des Softwareentwicklungsprozesses ■ Protokollierung administrativer Systemzugriffe ■ Dokumentation von Konfigurationsänderungen ■ Regelmäßige Überprüfung der Zugangsberechtigungen ■ Betrieb eines separaten Gast-Netzwerks (Gast-WLAN) ■ Einsatz server- und clientseitiger Spamfilter und Antimalwareprogramme (inkl. automatischer Updates) ■ Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe). ■ Automatisches Netzwerkmonitoring mit Alarmierung. ■ Abschaltung/Sperrung nicht benötigter Dienste und Netzwerkports.
3. Zugriffskontrolle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	■ Automatische Prüfung der Zugriffsberechtigung mittels Passwort ■ Ausschließliche Menüsteuerung je nach Berechtigung ■ Aufgaben- und Rollenbasiertes Berechtigungskonzept ■ Trennung von Anwendungs- und Administrationszugängen ■ Externer administrativer Zugriff nur im Ausnahmefall und unter Aufsicht von berechtigtem Personal ■ Durchführung regelmäßiger Softwareupdates ■ Automatisierte Vulnerability Scans als Teil des Softwareentwicklungsprozesses ■ Protokollierung administrativer Systemzugriffe ■ Dokumentation von Konfigurationsänderungen ■ Personenbezogene Daten, die im Auftrag verarbeitet werden, werden mit geeigneten

	Verschlüsselungsverfahren nach dem geltenden Stand der Technik verschlüsselt gespeichert ■ Zugriff auf Backups nur für Administratoren möglich ■ Backups werden mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik verschlüsselt ■ Löschung und Vernichtung von Datenträgern gemäß BSI-Empfehlungen
4. Trennungsgebot Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	■ Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden voneinander getrennt verarbeitet ■ Trennung von Test- und Produktionsumgebungen ■ Trennung Managementnetz von Produktionsnetz ■ Daten, die im Auftrag verarbeitet werden, werden für jeden Auftraggeber separat auf eigenständigen, getrennten Systemen verarbeitet
INTEGRITÄT	
1. Weitergabekontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	■ Übermittlung personenbezogener Daten mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik (mind. TLS 1.2, AES256) ■ Verschlüsselung von mobilen Endgeräten mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik ■ Löschung und Vernichtung von Datenträgern gemäß BSI-Empfehlungen
2. Eingabekontrolle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	■ Protokollierung zur nachträglichen Überprüfung der Datenverarbeitung(ssysteme) von: - erfolgreiche und gescheiterte An- und Abmeldevorgänge - Firewall-Protokollierung (TCP/IP) - Protokollierung administrative Tätigkeiten über Ticketsystem ■ Aufbewahrungsfristen für Backups sind festgelegt
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO) Maßnahmen, die gewährleisten, dass personenbezogene Daten	■ Alle Datenverarbeitungsanlagen, auf denen personenbezogene Daten gespeichert werden, verfügen über redundant eingebaute Festplattenspeicher (RAID)

gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.	■ Stromversorgungseinrichtungen der Serverräume (Stromkreise, USV-Anlagen, Netzteile) sind redundant ausgelegt ■ Im Falle eines Stromausfalls, der die mittels USV überbrückbare Zeitspanne übersteigt, werden alle Systeme automatisch kontrolliert heruntergefahren ■ Klimatisierung der Serverräume ■ Automatisierte Überwachung der gesamten Anlage auf Verfügbarkeit und ordnungsgemäßen Betrieb ■ Protokollierung und Meldung abnormer Ereignisse an zuständige Mitarbeiter ■ Gefahrenmeldeanlage für Brandausbruch, Wassereintritt, abnorme Klimaverhältnisse in den Serverräumen ■ Notfallplan wird im Alarmfall rund um die Uhr durch ein damit beauftragtes externes Werkschutzunternehmen umgesetzt ■ Zur ersten Brandbekämpfung sind geeignete Handfeuerlöscher installiert ■ Sicherung personenbezogener Daten erfolgt mindestens täglich auf ein eigenständiges, unabhängiges Backupsystem ■ Automatische Funktionsüberwachung der Datensicherung ■ Regelmäßige, stichprobenartige Prüfung der Wiederherstellbarkeit der Daten ■ Antimalwareprogramme sind vorhanden und werden immer auf dem aktuellsten Stand gehalten

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

1. Datenschutz-Management

Ein Datenschutzmanagementsystem ist umgesetzt. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen.

2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

3. Auftragskontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur	■ iS2-Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres

entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert. ■ Sollte iS2 bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden technisch-organisatorische Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO und Art 32 Abs. 1 DSGVO sichergestellt. ■ Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses: ■ Vertrag zur Auftragsverarbeitung nach Vorgabe Art. 28 Abs. 3 DSGVO ■ Datenverarbeitung erfolgt ausschließlich innerhalb der EU, bevorzugt in Deutschland ■ Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse ■ Wenn möglich Zertifizierung der Dienstleister nach ISO27001:2005 ■ Prüfungen und Audits der mit dem Dienstleister vereinbarten Maßnahmen ■ Auf technische Umgebungen von Dienstleistern werden Zugriffsberechtigungen für iS2-Mitarbeiter restriktiv vergeben. ■ Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.
PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG (Art. 32 Abs. 1 lit. a DSGVO)	
Einsatz verschiedener Verschlüsselungs-Instrumente (bspw. VPN, WLAN-Verschlüsselung, sicherer File-Transfer)	