Vertrag zur Auftragsdatenverarbeitung nach Art. 28 Abs. 3 DSGVO

Als Anlage zum Dokument „**547-ITD3.7078-2021 EVB-IT Dienstvertrag.pdf**“ vom [/]

zwischen dem Land Nordrhein-Westfalen,
vertreten durch das Ministerium der Justiz des Landes NRW,
vertreten durch den Präsidenten des Oberlandesgerichts Köln,
Zentraler IT-Dienstleister der Justiz des Landes NRW,
Dezernat ITD3 –Verträge und Beschaffung-

- im Auftrag der Arbeitsgruppe „IT-Standards in der Justiz“
der Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) -

Reichenspergerplatz 1, 50670 Köln

- nachfolgend „Auftraggeber“ –

und

der Fa. Procilon GmbH
Leipziger Straße 110
04425 Taucha

- nachfolgend „Auftragnehmer“ –
- beide nachfolgend gemeinsam „Vertragsparteien“ –

wird der folgende Vertrag geschlossen:

Präambel

Der Auftraggeber beabsichtigt den Auftragnehmer mit den in § 2 genannten Leistungen zu beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Vertrag zur Auftragsdatenverarbeitung, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DS-GVO definiert werden, sind im Sinne der gesetzlichen Definition zu verstehen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Umwandlung und des Versands von DE-Mail-Nachrichten von und zur EGVP-Infrastruktur der Justiz auf Grundlage des Vertrags mit der Vertragsnummer 547-ITD3.7078-2021 vom 27.06.2022 („Hauptvertrag“).

Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag nebst den zugehörigen Anlagen. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO.

(2) Zur Konkretisierung der datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den vorliegenden Vertrag. Dessen Regelungen gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrags finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt.

§ 4 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags verarbeitet der Auftragnehmer DE-Mail Adressen, Betreffzeilen, Nachrichten-IDs, Vor- und Nachnamen von DE-Mail Inhabern, Eingangszeitpunkt von DE-Mails sowie Inhalt von DE-Mails oder mittels DE-Mail ein- oder ausgehender Dokumente. Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst Verfahrensbeteiligte sowie weitere Personen entsprechend dem Vortrag der Parteien und den Erhebungen der weiteren Beteiligten, z.B. Sachverständige.

§ 5 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Weisungsberechtigt ist der Vorsitzende der BLK-AG IT-Standards oder weitere von diesem schriftlich benannte Personen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

(5) Seitens des Auftraggebers sind weisungsbefugt:

- [redacted]
- [redacted]

(6) Seitens des Auftragnehmers sind zur Entgegennahme von Weisungen befugt:

- [redacted]
- [redacted]

§ 6 Schutzmaßnahmen des Auftragnehmers

(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 sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die im **Anhang technische organisatorische Maßnahmen** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter [redacted] benannt.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrags betraut werden (im folgenden Beschäftigte genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrags oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

(5) Die Verarbeitung von Daten, die Gegenstand dieses Vertrags sind in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicherzustellen. Die Einhaltung der Schutzmaßnahmen nach § 6 Absätzen 1 und 2 dieses Vertrags sowie der Maßgaben des Art. 32 DS-GVO ist auch in diesem Fall sicherzustellen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:
   a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
   b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
   c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO).

Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 5 dieses Vertrags durchführen.

(5) 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegen.

(6) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 dieses Vertrags hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(7) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(8) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(9) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DS-GVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers, die die Verarbeitung von personenbezogene Daten aus dem Hauptvertrag und diesem AVV betreffen. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung des Subunternehmers [redacted] durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis") befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischem Format zugestimmt hat. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung

von Subunternehmern diese entsprechend den Regelungen dieses Vertrags zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus diesem Vertrag (insbesondere seine Prüf- und Kontrollrechte) wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis 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 Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS- GVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

(2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die allein daraus resultieren, dass der Auftragnehmer seinen speziell auferlegten Pflichten aus der DSGVO oder diesem Vertrag nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. Der Auftraggeber verpflichtet sich, im Innenverhältnis den Auftragnehmer von allen Ansprüchen Dritter freizustellen, die daraus resultieren, dass eine Verletzung dieses Vertrages und/oder gesetzlicher datenschutzrechtlicher Bestimmungen allein oder überwiegend auf ein Verhalten des Auftraggebers zurückzuführen ist.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO.

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrags der des Hauptvertrages.

§ 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine rechtmäßig erteilte Weisung des Auftraggebers nicht ausführen will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt, und wenn der Auftragnehmer nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats, den vertrags- bzw. rechtswidrigen Zustand beendet. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Der vorliegende Vertrag bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Dieser Vertrag unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Stuttgart.

28.06.2022, Stuttgart
Datum, Ort

[redacted]

Unterschrift (Auftraggeber)

[redacted]

Name, Vorname, Funktion

28.06.2022, Taucha

[redacted]

[redacted]

Name, Vorname, Funktion

Anhang „Technisch-organisatorische Maßnahmen

zur Vereinbarung zur Auftragsdatenverarbeitung vom 28.06.2022

Nr.	Maßnahme	Umsetzung der Maßnahme
1	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	Der Betrieb der Lösung erfolgt in einem nach ISO 27001/20018 konformen Rechenzentrum mit Datenstandort Deutschland. Der Zutritt zu der physischen Hardware ist durch ein technisches Zutrittskontrollsystem gesichert. Über Sicherheitssysteme (Alarmanlage, Wachschutz, etc.) wird die Infrastruktursicherheit gewährleistet.
2	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Da es sich bei dem System um einen Verbund von automatisierten Prozessen handelt, haben Endbenutzer keinen Zugriff auf die Infrastruktur. Die mit Administration beauftragten Mitarbeiter sind mit personalisierten und zertifikatsbasierten Zugängen ausgestattet. Die Berechtigungen werden in einem zentralen Verzeichnisdienst über Rollen vergeben. Der Zugriff wird protokolliert. Weiterhin werden die temporären Daten nach Stand der Technik verschlüsselt gespeichert.
3	**Zugriffskontrolle** Es ist zu 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.	Der Zugriff auf die Systeme wird gemäß Nr. 2 geregelt. Die Nachrichten werden nicht separat gespeichert, sondern auf den jeweiligen Quellsystemen abgeholt (DMDA) und auf die Zielsysteme (Intermediär) übertragen. Im Rahmen der Fehlerbehandlung kann es möglich sein, dass Nachrichten in einer Fehlerqueue liegen und nach einem Retry wieder in die Verarbeitung gebracht werden. Nach Erreichen der max. Wiederholversuche bzw. dem erfolgreichen Übermitteln werden die Daten gelöscht. Der Fehlerspeicher ist nach Stand der Technik verschlüsselt.
4	**Weitergabekontrolle** Es ist zu 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.	Die Übertragung erfolgt stets verschlüsselt. Zusätzlich wird für die temporäre Queue Verwaltung eine Festplattenverschlüsselung nach dem Stand der Technik eingesetzt. Systembackups werden nur von Systemkonfigurationen und Loginformationen angefertigt und sind ebenfalls stets verschlüsselt.
5	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme	Zur Nachvollziehbarkeit werden personalisierte Accounts der Operatoren verwendet. Neben der Systemprotokollierung werden auch die Zugänge zum System organisatorisch überwacht. Die Logfiles werden wie alle anderen Daten verschlüsselt.

	eingegeben, verändert oder entfernt worden sind.	
6	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Die Transformation der De-Mail nach EGVP und von EGVP zu DE-Mail Nachrichten basiert auf den vertraglichen Grundlagen zwischen Auftraggeber und Auftragnehmer. Solange dieser Vertrag Bestand hat, werden die Nachrichten in jeweils beide Richtungen, gemäß der Auftragsbeschreibung umgesetzt. Es handelt sich dabei um einen vollautomatischen Prozess mit Überwachungsfunktion. Die Pflege der Teilnehmer erfolgt über SAFE. Der Auftragnehmer hat damit keinen Einfluss auf den Nachrichtenfluss. Nach Weisung des Auftraggebers kann der Dienst jederzeit abgeschaltet werden.
7	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Im Rahmen der Vertragserfüllung stellen sich folgende Aufgaben zur Absicherung der Verfügbarkeit: Die Adressdaten liegen in SAFE und werden in das Auftragsdatenverarbeitungssystem nicht synchronisiert, sondern über die verfügbaren Schnittstellen des SAFE Systems abgefragt. Die DE-Mails liegen im System des DMDA und werden direkt an den Empfänger ins EGVP übertragen. Bei fehlerhaften Nachrichten bzw. der Nichtverfügbarkeit der Umsysteme (SAFE, Intermediäre) werden die Nachrichten nur temporär zwischen gepuffert. Der Datenträger ist hochverfügbar (redundant) und verschlüsselt. Alle Infrastruktursysteme sind ebenfalls redundant ausgelegt und können bei Bedarf zur Skalierung beitragen. Weiterhin werden regelmäßig verschlüsselte Systembackups durchgeführt. Da die Nachrichtenquittierung erst bei erfolgreicher Zustellung erfolgt, sind die Daten auf den Quellsystemen noch abrufbar. Das Gateway stellt keine eigene Postbox im eigentliche Sinne dar, sondern agiert als Nachrichtenrouter zwischen den sicheren Übermittlungswegen.
8	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Es wird eine strikte Systemtrennung zwischen den Systemkomponenten durchgeführt. Für die Test- und Produktionsumgebungen werden eigene Ressourcengruppen angelegt. Der Zugriff auf diese Ressourcengruppe ist Netz- und Firewall technisch unterbunden. Eine Verzeichnisdienstkombination zwischen SAFE Produktion und Test ist nicht zulässig. Für die EGVP Postfachadressierung und die DE-MAIL Domain wird eine Unterscheidung und damit getrennte Konfiguration in den jeweiligen Ressourcengruppen verwendet.

28.06.2022, Stuttgart

Datu[redacted]

Unterschrift (Auftraggeber)

[redacted]

Name, Vorname, Funktion

28.06.2022, Taucha

[redacted]

Name, Vorname, Funktion