Rahmenverwaltungsvereinbarung
zum Aufbau und Betrieb der IT für das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen

zwischen dem

Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen
Krausenstr. 17 - 18
10117 Berlin

- im Folgenden „BMWSB“ oder „Auftraggeber“ (AG) genannt -

und dem

Bundesministerium der Finanzen
Wilhelmstraße 97
10117 Berlin

- im Folgenden „BMF“ genannt -

als zuständigem Ressort für das

Informationstechnikzentrum Bund
Bernkasteler Straße 8
53175 Bonn

- im Folgenden „ITZBund“ oder „Auftragnehmer“ (AN) genannt -

- BMWSB und ITZBund gemeinschaftlich im Folgenden „Parteien“ genannt -

Inhaltsverzeichnis

Präambel

Mit Organisationserlass der Bundesregierung wurde das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) zum 8. Dezember 2021 eingerichtet. In den Geschäftsbereich des BMWSB ist das Bundesamt für Bauwesen und Raumordnung (BBR) gewechselt, Regelungen hierzu werden zu einem späteren Zeitpunkt getroffen.

Das ITZBund übernimmt sukzessive, spätestens ab dem 23./24.07.2022, insgesamt als zentraler IT-Dienstleister die IT-seitige Betreuung des BMWSB, die bis dahin vom BMI wahrgenommen wird. Die Informationstechnik und die IT-Services für das BMWSB werden durch das ITZBund initial in 2022 eingerichtet und es werden nachfolgend Betrieb sowie Betreuung sichergestellt.

IT-Service und IT-Sicherheit entsprechen dem Standard des BMF. Entsprechend der für Ministerien bestehenden hohen Sicherheitsanforderungen sowie des Beschlusses des IT-Rates werden die Regierungsnetze, insbesondere NdB genutzt, und diese Anschlüsse werden - soweit nicht von der BDBOS verantwortet - vom ITZBund betreut. Die Migration von P 2 auf P 3 inklusive der Überführung der gesamten Netzdienstleistungen auf die Infrastruktur der BDBOS (NdB) wird schnellstmöglich angestrebt, das BMWSB wird sich mit dem BMI abstimmen.

Diese Rahmenverwaltungsvereinbarung (RVV) beschreibt den Regelungsrahmen der Zusammenarbeit zwischen dem BMWSB und dem ITZBund sowohl im Rahmen der initialen Umsetzung als auch im späteren Regelbetrieb. Sie ordnet sich in die bestehende ressortübergreifende IT-Steuerung bzw. -Organisation des Bundes ein. In diesem Rahmen wirken die Behörden zusammen auf Grundlage der öffentlich-rechtlichen Vorschriften im Rahmen der hoheitlichen Aufgabenwahrnehmung. Hierzu knüpft diese RVV gemäß der gesetzlichen Zuweisung der zentralen Aufgabenzuständigkeit im Bereich der IT-Verwaltung und IT-Konsolidierung der Bundesverwaltung zum ITZBund als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums der Finanzen an das bundesverwaltungsspezifische „Auftraggeber-/Auftragnehmer-Modell“ (vgl. § 2 Abs. 6 ITZBundG) an. Dieses unterliegt einem öffentlich-rechtlichen Verständnis im Rahmen der gemeinsamen hoheitlichen Aufgabenwahrnehmung unter Sicherstellung der Hoheit, Kontrollfähigkeit und Sicherheit der erforderlichen Verfahrensabläufe an den behördenübergreifenden Schnittstellen und Aufgabenzuständigkeiten der Verwaltung. In diesem gesetzlich vorgegebenen Rollenmodell werden bezeichnet

- als „Auftraggeber“ („AG“) die Behörden / Ressorts, die bzw. deren Fachreferate („Bedarfsträger“) zur (gemeinsamen) hoheitlichen Aufgabenwahrnehmung auf IT-Dienste und Ressourcen der Bundesverwaltung angewiesen sind (hier das BMWSB),
- als „Auftragnehmer“ („AN“) das ITZBund als für die IT-Verwaltung und IT-Konsolidierung des Bundes maßgeblicher Aufgabenträger (vgl. § 2 ITZBundG).

§ 1
Gegenstand und Umfang der Rahmenverwaltungsvereinbarung

(1) Diese Rahmenverwaltungsvereinbarung (RVV) definiert die übergreifenden Regelungen für die Erbringung von IT-Leistungen für das BMWSB durch das ITZBund.

(2) Neben und auf Grundlage der RVV werden jeweils folgende weiteren Verwaltungsvereinbarungen zwischen dem Auftraggeber und dem Auftragnehmer abgeschlossen, die die jeweiligen konkreten Pflichten und den Aufgabenumfang festlegen:

a) „Abgestimmter Liefer- und Leistungsumfang zur initialen Umsetzung der IT-Anforderungen des BMWSB“,
b) „Vereinbarungen gemäß den Gemeinsamen Geschäftsbedingungen zur Zusammenarbeit mit dem ITZBund (GGB)“ (vgl. Anlage 1, in der Regel „Service Level Agreements (SLA)“) zur konkreten vereinbarten Ausgestaltung der übernommenen IT-Aufgaben im Regelbetrieb (z.B. Servicescheine „IT-Arbeitsplatz“, „Sondersupport“, „Bundescloud“, „E-Akte“).
c) Daneben können weitere ergänzende Vereinbarungen abgeschlossen werden.

§ 2
Geltungsreihenfolge

Für die Zusammenarbeit zwischen BMWSB und ITZBund gilt die folgende Geltungsreihenfolge:

a) diese RVV,
b) Gemeinsame Geschäftsbedingungen des ITZBund (GGB), vgl. **§ 4 Abs. 2 i. V. m. Anlage 1** und
c) Vereinbarung nach **§ 1 Abs. 2 lit. b-c**

§ 3
Initiale Einrichtung der IT des BMWSB

(1) Die Parteien arbeiten während der initialen Einrichtung der IT-Struktur und der damit zusammenhängenden IT-Maßnahmen eng zusammen, um die Erstausstattung des BMWSB sicherzustellen. Im ITZBund wird dazu ein Projekt eingerichtet.

(2) Die initiale Einrichtung umfasst

a. die Erstausstattung der Beschäftigten des BMWSB mit IT-Arbeitsplätzen einschließlich erforderlicher Bürokommunikationssoftware und im Rahmen von mobilen Smartdevices und IT-Veranstaltungsunterstützung der erforderlichen Endgeräte (einschließlich Telefonendgeräte) sowie die initiale Einrichtung der Fachverfahren,
b. die initiale Einrichtung der Prozesse für IT-Betreuung dieser IT-Arbeitsplätze, Telefonie und Endgeräte einschließlich Service Desk,
c. die für den IT-Betrieb erforderliche Backend-Infrastruktur in einem Rechenzentrum des ITZBund und in den Liegenschaften des BMWSB

(3) Das ITZBund kann einzelne IT-Leistungen unterbeauftragen. Zur Unterbeauftragung gilt:

a) Das ITZBund darf Dritte (Unterauftragnehmer) mit der Erbringung von Teilleistungen beauftragen (Zulieferleistungen).

b) Eine Unterbeauftragung ändert nichts an der vereinbarten Verpflichtung der Parteien zur Erbringung der jeweiligen Teilleistungen. Handlungen der Unterauftragnehmer sind wie eigene zu vertreten.

c) Unterauftragnehmerleistungen werden nur an geeignete (fachkundige, leistungsfähige, zuverlässige und erfahrene) Unterauftragnehmer vergeben. Unterauftragnehmer müssen in Bezug auf ihren Leistungsanteil mindestens über gleichwertige Qualifikationen wie das ITZBund und über die nach dem Gesetz oder in dieser RVV genannten erforderlichen Genehmigungen, Zulassungen und Ermächtigungen verfügen.

d) Das ITZBund wird dem BMWSB vor Abschluss einer Vereinbarung nach **§ 1 Abs. 2 lit. b-c** eine Übersicht über die im ITZBund eingesetzten Unterauftragnehmer zur Verfügung stellen. Das ITZBund wird das BMWSB rechtzeitig vor Aufnahme der Tätigkeit des jeweiligen Unterauftragnehmers in gleicher Form über Veränderungen unterrichten.

e) Die Unterauftragnehmer werden vom ITZBund verpflichtet, die datenschutzrechtlichen Regelungen ihres Auftraggebers (ITZBund) vollumfänglich einzuhalten. Vor der Beauftragung Dritter durch das ITZBund ist die Zustimmung des BMWSB einzuholen[1].

§ 4
Regelbetrieb

(1) Das BMWSB arbeitet im Regelbetrieb mit dem ITZBund in einem Auftraggeber-/ Auftragnehmer-Modell zusammen.

(2) Die Regelungen zur Zusammenarbeit in diesem Auftraggeber- / Auftragnehmer-Modell ergeben sich aus den „Gemeinsamen Geschäftsbedingungen zur Zusammenarbeit mit dem ITZBund (GGB)“ in der jeweils gültigen Fassung. Die Fundstelle der aktuellen Version ist als **Anlage 1** beigefügt.

(3) Für die Zusammenarbeit mit dem ITZBund richtet das BMWSB eine zentrale Rolle (Fach-Auftraggeberschnittstelle) in seiner Organisation ein. Zusätzlich wird die Rolle einer koordinierenden Ressort-Auftraggeberschnittstelle eingerichtet. Die Aufgaben der Ressort- und Fachauftraggeberschnittstelle können in einer gemeinsamen Organisationseinheit wahrgenommen werden. Die Aufgaben der Auftraggeberschnittstellen sind in den GGB beschrieben.

(4) Das BMWSB schließt mit dem ITZBund zu allen von diesem zu erbringenden IT-Leistungen im Regelbetrieb gesonderte Einzelaufträge und/oder SLA ab.

(5) ITZBund und BMWSB werden gemäß DSGVO eine Vereinbarung zur Auftragsverarbeitung abschließen (vgl. Anlage 2).

(6) Eine Unterbeauftragung richtet sich nach den getroffenen Vereinbarungen zur Auftragsverarbeitung.

[1] Siehe Anlage 2: „Bundes-Mustervereinbarung zur Auftragsverarbeitung mit dem ITZBund nebst Nebenabreden“

(7) Das BMWSB und das ITZBund können in den jeweiligen „Vereinbarungen gemäß den Gemeinsamen Geschäftsbedingungen zur Zusammenarbeit mit dem ITZBund (GGB)“ nach **§ 1 Abs. 2 lit. b** Regelungen treffen zum Einsatz von Unterauftragnehmern für behördenspezifische Lösungen sowie zu den Unterauftragnehmern, die Zutritt zu den Liegenschaften des BMWSB erhalten.

(8) Beide Parteien stellen sicher, dass der Zutritt und Zugang[2] zu den durch den Auftragnehmer zu betreuenden IT-Systemen innerhalb der vereinbarten Zeiten möglich sind.

(9) Für die Aufgabenerledigung sowie aus Gründen der IT-Sicherheit/VS-NfD-Konformität wird dem Auftragnehmer grundsätzlich die vollständige Verfügungsgewalt über die von ihm zu betreuende Infrastruktur sowie der Zugang zu davon betroffenen Räumlichkeiten eingeräumt. Sofern diese in anderen Liegenschaften als denen des BMWSB liegen, wird durch dieses ein uneingeschränkter Zugang sichergestellt.

§ 5
Finanzierung

(1) Ausgaben für die initiale Einrichtung der Arbeitsplatz-IT einschließlich Endgeräten und Maßnahmen gem. § 3 Abs. 2 a) werden durch das BMWSB finanziert.

(2) Die Finanzierung der Ausgaben für die in § 3 Abs. 2 b) genannten Maßnahmen sowie die erforderliche Backend-Infrastruktur zu den in Abs. 1 genannten Arbeitsplätzen und Geräten (§ 3 Abs. 2 c) erfolgt durch das ITZBund.

(3) Die Finanzierung der Ausgaben im Regelbetrieb richtet sich nach der jeweils aktuellen Version der GGB (vgl. **§ 4 Abs. 2**).

§ 6
Allgemeine Pflichten des Auftragnehmers für den Regelbetrieb

(1) In Bezug auf den Regelbetrieb erbringt der Auftragnehmer die Dienstleistungen nach Maßgabe von **§ 4**. Er wird dabei seine in den GGB festgelegten Aufgaben an der Kundenschnittstelle wahrnehmen.

(2) Der Auftragnehmer erbringt die Dienstleistung nach den aktuellen gesetzlichen Regelungen und Verordnungen sowie dem aktuellen Stand der Technik und durch Personal, das für die Erbringung der vereinbarten Leistungen qualifiziert ist.

(3) Der Auftragnehmer trägt Sorge für eine stabile und wirtschaftliche Leistungserbringung für das BMWSB.

[2] BSI: Glossar der Cybersicherheit, letzter Aufruf am 29.10.2021,

§ 7
Allgemeine Rechte und Pflichten des Auftraggebers für den Regelbetrieb

(1) Das BMWSB erhält Sitz und Stimmrecht im Verwaltungsrat und im Kundenbeirat des ITZBund.

(2) Das BMWSB wird im Regelbetrieb die in den GGB festgelegten Aufgaben an der Kundenschnittstelle wahrnehmen.

(3) Das BMWSB erbringt die jeweils vereinbarten Mitwirkungs- und Beistellleistungen (vgl. **§ 1 Abs. 2**). Es unterstützt das ITZBund im vereinbarten Umfang und stellt alle in diesem Zusammenhang notwendigen Informationen zur Verfügung.

(4) Die aus den Dienstvereinbarungen des BMWSB folgenden organisatorischen und technischen Anforderungen an das ITZBund einschließlich Informations-, Auskunfts- und Kontrollrechte der Gleichstellungsbeauftragten und der Interessenvertretungen gegenüber dem BMWSB werden in den Vereinbarungen nach **§ 1 Abs. 2 lit. c** geregelt.

§ 8
Informationssicherheit, Datenschutz und Geheim- und Sabotageschutz

(1) Das Verhältnis zwischen den Parteien entspricht einem Outsourcing-Verhältnis nach dem BSI IT-Grundschutz. Das BMWSB und das ITZBund stellen für ihren jeweiligen Zuständigkeitsbereich sicher, dass die Vorgaben zur Informationssicherheit (insbesondere BSIG, UP Bund, BSI IT-Grundschutz, BSI-Mindeststandards in der jeweils geltenden Fassung), zum Datenschutz (insbesondere Art. 28, 29 DSGVO) und zum Geheim- und Sabotageschutz (insbesondere SÜG, VSA) angemessen und wirksam implementiert und über die gesamte Dauer der Vereinbarung lückenlos aufrechterhalten werden. Die notwendigerweise zu schließenden Vereinbarungen zur Auftragsverarbeitung orientieren sich an **Anlage 2**.

(2) Eine wesentliche operative Grundlage für das Informationssicherheitsmanagement stellen zudem die GGB (vgl. **§ 4 Abs. 2**) in der jeweils geltenden Fassung dar.

(3) Das BMWSB und das ITZBund einschließlich seiner Rechts- und Fachaufsicht sind verpflichtet, alle erlangten Informationen vertraulich zu behandeln und nur zum vereinbarten Zweck zu nutzen. Diese Verpflichtung gilt auch über die Beendigung dieser RVV hinaus.

(4) Das ITZBund gewährleistet, dass die dem BMWSB bereitgestellten IT-Lösungen und IT-Services gemäß den Vorgaben zur Informationssicherheit konfiguriert und betrieben, auf dem aktuellen Stand der Technik gehalten und die dafür erforderlichen Dokumentationen erstellt werden. Dies bedarf einer Vereinbarung nach **§ 1 Abs. 2 lit. b**. Diese Vereinbarung umfasst auch die Bereitstellung entsprechender, mandantenspezifischer Dokumentationstools mit Zugriffsmöglichkeiten für das BMWSB auf die durch das ITZBund bereitgehaltenen Informationen.

(5) Zugriffs- und Datenherausgabeberechtigungen bzw. -beschränkungen werden in den Vereinbarungen nach **§ 1 Abs. 2 lit. b** geregelt.

§ 9
Notfall- und Krisenmanagement

(1) ITZBund und BMWSB werden für den Regelbetrieb ein Notfall- und Krisenmanagement gemäß BSI IT-Grundschutz implementieren Dies umfasst sowohl die Notfallvorsorge als auch die Notfallbewältigung für beide Parteien.

(2) Die konkrete Ausgestaltung der Anforderungen an das Notfall- und Krisenmanagement vereinbaren das BMWSB und der Auftragnehmer im Rahmen von SLA-Vereinbarungen nach **§ 1 Abs. 2 lit. b**.

§ 10
Schutzrechte[3]

(1) Das BMWSB und das ITZBund treffen Regelungen über Nutzungsrechte im Rahmen ihrer Vereinbarungen nach **§ 1 Abs. 2 lit. b**.

§ 11
Verantwortliche Ansprechpersonen

(1) Ein gemeinsames Verständnis über die in dieser RVV oder darüber hinaus getroffenen Vereinbarungen (vgl. **§ 1 Abs. 2 lit. b-c**) ist Voraussetzung für die Erfüllung der gestellten Anforderungen. Zu diesem Zweck benennen der Auftragnehmer und das BMWSB die jeweils zuständigen Ansprechpersonen:

   a) Für den Aufbau der Infrastruktur und die initiale Einrichtung der IT für das BMWSB ergeben sich die Ansprechpersonen aus der Projektorganisation der Parteien.

   b) Für den Regelbetrieb ergeben sich die Ansprechpersonen aus den jeweiligen Vereinbarungen gem. **§ 1 Abs. 2 lit. b und c**.

(2) Unabhängig von den vorstehenden Regelungen verpflichten sich alle Beteiligten, alle für die Aufgabenerledigung wichtigen Informationen, insbesondere geänderte Zuständigkeiten, Vertretungsregelungen sowie Prozess- oder Verfahrensänderungen, zeitnah mitzuteilen.

§ 12
Eskalation

(1) Bei einer Eskalation während der initialen Einrichtung der IT des BMWSB (Projekt) ist der Steuerungskreis die erste Eskalationsinstanz. Wird kein Einvernehmen erzielt, ist der Lenkungsausschuss die zweite und letzte Eskalationsinstanz. Näheres zum Eskalationsmechanismus ist im Projekthandbuch des gemeinsamen Projekts geregelt.

(2) Eine Eskalation im Regelbetrieb erfolgt nach den Regelungen der GGB.

[3] auch Intellectual Property (IP)

§ 13
Dauer, Anpassung und Kündigung der Vereinbarung

(1) Diese RVV tritt mit Unterzeichnung in Kraft und wird auf unbestimmte Zeit geschlossen.

(2) Eine Anpassung sowohl der RVV als auch ihrer Anlagen ist jederzeit bei beiderseitigem Einverständnis möglich. § 14 Abs. 2 ist zu beachten.

(3) Beide Seiten können diese Vereinbarung schriftlich mit einer Frist von 24 Monaten zum Ende eines Kalenderjahres kündigen. In der Kündigungserklärung sollen die Gründe für die Kündigung dargelegt werden. Eine außerordentliche Kündigung ist möglich, wenn ein weiteres Festhalten an dieser Vereinbarung nicht zumutbar ist. Die Vereinbarungen nach **§ 1 Abs. 2 lit b-c** enden vorbehaltlich abweichender Regelungen zwischen dem BMWSB und dem ITZBund zum gleichen Zeitpunkt.

§ 14
Salvatorische Klausel, Auslegung, Formerfordernis

(1) Sollten einzelne Bestimmungen dieser Vereinbarung oder ihrer Anlagen teilweise oder vollständig nichtig oder aus anderen Gründen unwirksam sein oder sollte sich in dieser Vereinbarung und ihren Anlagen eine Regelungslücke herausstellen, bleiben die übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen Bestimmung soll eine angemessene Regelung gelten, die soweit möglich, dem am nächsten kommt, was beide Seiten gewollt haben würden, sofern sie diesen Punkt bedacht hätten. Im Falle einer Regelungslücke bemühen sich beide Seiten, sich so bald wie möglich auf eine geeignete Regelung zu verständigen und diese unter Beachtung von Absatz 2 in einem Nachtrag zu dieser Vereinbarung zu dokumentieren.

(2) In dieser Rahmenverwaltungsvereinbarung (RVV), dazugehörigen Anlagen oder sonstigen auf Grundlage dieser RVV ergehende Vereinbarungen und Regelungen sowie verwendete Begrifflichkeiten, Rollenbezeichnungen der beteiligten Behörden nebst ihren Zuständigkeiten und Verantwortlichkeiten ordnen sich dem öffentlich-rechtlichen Verständnis der hoheitlichen Aufgabenwahrnehmung unter und sind ausschließlich auf öffentlich-rechtlicher Grundlage gemäß den gesetzlichen und verwaltungsrechtlichen Vorgaben im Rahmen des Organisationsverständnisses der Bundesverwaltung zu verstehen und anzuwenden.

(3) Änderungen und Ergänzungen dieser Vereinbarung und ihrer Anlagen, einschließlich dieser Klausel, bedürfen zu ihrer Wirksamkeit der Schriftform.

Ort *Datum*	Berlin, 9.8.2022 *Ort* *Datum*
Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen *vertreten durch,* ***Name, Titel***	**Bundesministerium der Finanzen** *vertreten durch,* ***Name, Titel***
(Unterschrift)	(Unterschrift)

Steffen Saebisch
Staatssekretär
Bundesministerium der Finanzen
Wilhelmstraße 97, 10117 Berlin
Telefon: 030 18682-4534
Fax: 030 18682-4440
E-Mail: Steffen.Saebisch@bmf.bund.de

Anlagenverzeichnis

Anlage 1 Fundstelle Gemeinsame Geschäftsbedingungen zur Zusammenarbeit mit dem ITZBund (GGB)

Anlage 2 Bundes-Mustervereinbarung zur Auftragsverarbeitung mit dem ITZBund

Anlage 1 -
Fundstelle Gemeinsame Geschäftsbedingungen zur Zusammenarbeit mit dem ITZBund (GGB)

Die jeweils aktuelle Fassung der GGB wird unter folgendem Link veröffentlicht:

https://social.intranet.bund.de/inhalte/Aufgabe_202

Die derzeit geltende Fassung der GGB ist die Version 2022_1 vom 12

Anlage 2

Informations
Technik
Zentrum Bund

Vereinbarung zur Auftragsverarbeitung

AV-Referenznummer:

zwischen dem

< Kunde >

- nachfolgend „Verantwortlicher“ -

und dem

Informationstechnikzentrum Bund
Bernkasteler Straße 8
53175 Bonn

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Konkretisierung des Auftragsinhaltes

(a) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung in ihrer jeweils gültigen Fassung.

(b) Die Datenarten oder -kategorien, die Gegenstand der Verarbeitung durch den Auftragsverarbeiter sind, bestimmen sich nach Anlage 2.

(c) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist in Anlage 2 konkret beschrieben.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(a) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(b) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(c) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(d) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der

Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung sowie diese Vereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(e) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in Anlage 2 festgelegt.

(f) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(g) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(h) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig, wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(i) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z. B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(a) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(b) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(c) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der/des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(d) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(a) Die Vertragsparteien vereinbaren die in der Anlage 3 zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Die Anlage ist Gegenstand dieser Vereinbarung.

(b) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in der Anlage 3 festgelegten technisch-organisatorischen Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(c) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 DSGVO und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(d) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(e) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz d sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(f) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für die betroffene Person zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(a) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(b) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(c) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz b.

§ 8 Subunternehmen

(a) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen. Die zum Zeitpunkt des Vertragsschlusses zur Erfüllung hinzugezogenen Subunternehmen sind in der Anlage 2 im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden. Sofern es sich um eine allgemeine schriftliche Genehmigung handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(b) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(c) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortliche berechtigt, auf schriftliche oder per E-Mail übermittelte Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(d) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragen des Verantwortlichen sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht (hier: die/der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet

insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Schlussbestimmungen

(a) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung 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.

(b) Diese Vereinbarung wird als Rahmenvereinbarung bzgl. der in Anlage 2 aufgeführten Leistungsvereinbarung abgeschlossen.

(c) Weiterhin ist Bestandteil dieser Vereinbarung die Nebenabrede als Anlage 1 sowie sämtliche nachstehend aufgeführten Anlagen.

(d) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Verantwortlicher vertreten durch **< Kunde >**	Datum Unterschrift
Auftragsverarbeiter ITZBund vertreten durch Herrn RD Gilbert	Datum Unterschrift

Anlagen:

- Anlage 1 – Nebenabrede
- Anlage 2 – Leistungsvereinbarung

  Übersicht Leistungsvereinbarungen
  Anlagen Leistungsvereinbarungen
- Anlage 3 – TOM

Nebenabreden zur Vereinbarung zur Auftragsverarbeitung vom < TT.MM.JJJJ >

zu den Punkten

- § 2 – Konkretisierung des Auftragsinhaltes
- § 3 (h) und (i) – Verantwortlichkeit und Weisungsbefugnis
- § 8 (a) – Subunternehmen
- § 10 – Schlussbestimmungen

der Vereinbarung zur Auftragsverarbeitung vom < TT.MM.JJJJ >

zwischen dem

< Kunde >

- nachfolgend „Verantwortlicher“ -

und dem

Informationstechnikzentrum Bund
Bernkasteler Straße 8
53175 Bonn

- nachfolgend „Auftragsverarbeiter“ -

Präambel

Mit der Vereinbarung der nachfolgenden Nebenabreden tragen die Vertragsparteien der besonderen Stellung des generalunternehmerischen Auftragsverarbeiters ITZ-Bund als IT-Dienstleister der Bundesverwaltung Rechnung. Die Abreden ergänzen bzw. konkretisieren die Vereinbarung über die Auftragsverarbeitung (im Folgenden: AV). Die Geltungsreihenfolge ist:

1. AV,
2. diese Nebenabrede,
3. sonstige Anlagen.

Zu § 2 – Konkretisierung des Auftragsinhaltes

Die Vereinbarung umfasst eine Zusammenstellung aller Leistungsvereinbarungen zwischen Verantwortlichem und Auftragsverarbeiter sowie die ggfls. vereinbarten verfahrensspezifischen Anforderungen , die nicht durch die Standard-TOM des ITZBund erfüllt werden, in der Anlage 2. Die Zusammenstellung der Leistungsvereinbarungen zur Auftragsverarbeitung sowie die ggfls. vereinbarten verfahrensspezifischen Anforderungen können einvernehmlich aktualisiert werden und gelten damit jeweils in der aktuellen Fassung als Bestandteil dieser Vereinbarung.

Zu § 3 (h) – Verantwortlichkeit und Weisungsbefugnis

Die Auftragsverarbeitung erfolgt auf der Grundlage der Definition des Art. 4 DSGVO ausschließlich auf dem Gebiet der Bundesrepublik Deutschland. Dies schließt (Fern-) Wartung und sonstige Fernzugriffe im Rahmen der Auftragsverarbeitung mit ein.

Zu § 3 (i) – Verantwortlichkeit und Weisungsbefugnis

(1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass ihnen unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Einer Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (Standard Mobilarbeitsplätze, z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) wird – vorbehaltlich anderslautender Weisungen auf Grundlage der/des DSGVO/BDSG – unter folgenden Bedingungen zugestimmt:

1. Die Standard-Telearbeitsplätze werden im Rahmen des jeweils freigegebenen Auftragsverarbeiter IT-Sicherheitskonzeptes betrieben.
2. Es findet außerhalb der Betriebsräume keine lokale Verarbeitung auf den APC statt.
3. Ein gesicherter Zugriff und eine darauffolgende Verarbeitung von personenbezogenen Daten auf Anwenderebene (Klarsicht) findet nur im Ausnahmefall und ausschließlich unter Zustimmung und nach Anweisungslage des Verantwortlichen i.S.v. Art. 4 Nr. 7 DSGVO statt.

4. Hierbei werden nur die Bildschirminformationen aus der Administrationsumgebung an die APC übermittelt. Eine lokale Speicherung und Verarbeitung erfolgt somit nicht.

(2) Soweit der Verantwortliche bezüglich der Leistungsvereinbarungen in Anlage 2 aufgrund eines voraussichtlich hohen Risikos der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen zur Durchführung einer Datenschutzfolgenabschätzung (DSFA; Art. 35 DSGVO) verpflichtet ist, ist eine Telearbeit erst nach Abschluss der DSFA unter Beachtung der daraus resultierenden Einschränkungen zulässig. Der Verantwortliche informiert den Auftragsverarbeiter jeweils unverzüglich über Bestehen oder Nichtbestehen einer DSFA-Pflicht und klärt mit ihm die zu treffenden Maßnahmen.

Bei der Verarbeitung von Daten, die höher als “VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft sind, sind Telearbeit und mobiles Arbeiten nicht zulässig.

(3) Die Vergabe eines Telearbeitsplatzes beim Auftragsverarbeiter basiert auf Eignungsprüfungen der Tätigkeiten für Telearbeit, den Eignungskriterien für Telebeschäftigte und der Eignung der Telearbeitsstätte. Insbesondere ist zu berücksichtigen, ob und inwieweit eine medienbruchfreie vollelektronische Verarbeitung möglich ist. Absatz 1 Ziffer 3 gilt entsprechend.

Zu § 8 (a) – Subunternehmen

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Inanspruchnahme weiterer Auftragsverarbeiter (Art. 28 Abs. 2 S. 1 DSGVO) für alle von dieser Vereinbarung erfassten Aufträgen des Verantwortlichen. Sofern auch Personalaktendaten durch weitere Auftragsverarbeiter verarbeitet werden sollen, gelten die speziellen Regelungen des § 111a Bundesbeamtengesetz (BBG). Die zum Zeitpunkt des Abschlusses der Vereinbarung zur Auftragsverarbeitung eingesetzten weiteren Auftragsverarbeiter (Subunternehmen) sind in Anlage 2 gesondert aufgeführt. Die Aufstellung umfasst auch die von den Subunternehmen ihrerseits in der jeweiligen Anwendung eingesetzten weiteren Subunternehmen.

(2) Die Information über beabsichtigte Änderungen im Zusammenhang mit bestehenden und zukünftigen weiteren Auftragsverhältnissen (§ 8 (a) der AV) bezüglich der in Absatz 1 bezeichneten Subunternehmen oder ihrer Rolle im Rahmen der Auftragsverarbeitung hat mit Kenntnis der Änderung unverzüglich, spätestens jedoch zwei Monate vor dem Änderungszeitpunkt schriftlich oder per E-Mail zu erfolgen. Die Zwei-Monats-Frist gilt nicht, soweit zwingende betriebstechnische Gründe eine kurzfristigere Änderung unumgänglich machen.

(3) Der Verantwortliche kann gegen Änderungen gemäß Absatz 2 Einspruch erheben. Der Einspruch ist nur zulässig, wenn

1. die Rechtsposition des Verantwortlichen nach dem Vertrag durch die Änderung verschlechtert wird,

2. der Verantwortliche begründeten Anlass zu Bedenken hinsichtlich der Einhaltung der gesetzlichen Pflichten des Datenschutzes und/oder der Informationssicherheit durch den jeweiligen Subunternehmer hat oder

3. tatsächliche Anhaltspunkte für ein nicht rechtskonformes Verhalten des Subunternehmers vorliegen, das geeignet ist, das Vertrauen in seine generelle Zuverlässigkeit zu erschüttern.

Der Einspruch muss datenschutzrechtlich relevant sein und substantiiert begründet werden.

Erhebt der Verantwortliche gegen den Einsatz eines Subunternehmens Einspruch, so klären der Verantwortliche und der Auftragsverarbeiter das weitere Vorgehen. Bis zur Klärung eines substantiiert vorgetragenen Einspruchs darf das betreffende Subunternehmen grundsätzlich nicht für die gegenständliche Anwendung eingesetzt werden.

(4) Zur Vermeidung von Kettenauslagerungen und einer unbestimmten Anzahl von weiteren Auftragsverarbeitern werden die weiteren Beauftragungen auf maximal drei begrenzt.

Zu § 10 – Schlussbestimmungen

(1) Die Vereinbarung tritt zum Zeitpunkt der Unterzeichnung in Kraft. Die AV tritt für die jeweilige Anwendung in Anlage 2 außer Kraft, wenn das zugrundeliegende Auftragsverhältnis zwischen den Parteien beendet ist.

(2) Diese Vereinbarung ersetzt alle bisherigen datenschutzrechtlichen Regelungen durch den Verantwortlichen bzgl. der von der Vereinbarung erfassten Leistungsvereinbarungen. Dies gilt nicht für Leistungsvereinbarungen deren verfahrensspezifische Anforderungen nicht durch die Standard -TOM des ITZBund erfüllt werden.

(3) Diese AV tritt außerdem außer Kraft, sofern die Vertragsparteien eine ersetzende Rahmen-Regelung zur Auftragsverarbeitung treffen, deren Anwendungsbereich die jeweilige Anwendung in Anlage 2 abdeckt.

Verantwortlicher vertreten durch **< Kunde >**	Datum
	Unterschrift
Auftragsverarbeiter ITZBund vertreten durch Herrn RD Gilbert	Datum
	Unterschrift

Verfahren: xy **SLA/Serviceschein: AKZ xy**

Anlass und Gegenstand der Auftragsverarbeitung	Kreis der Betroffenen	Auftragsdauer	Schutzbedarf
Bspw. Bereitstellung, Betrieb, Wartung, technischer Support des Verfahrens.	Bspw.: Mitarbeiter, Bewerber, Kunden, …	Bestimmtes Datum oder unbefristet?	Wählen Sie ein Element aus.

Kategorie der Daten	Beschreibung der Kategorie	Verarbeitungszweck der Kategorie	Verarbeitungsdauer der Kategorie
Bspw.: Identitätsdaten	Bspw.: Vorname, Name, Adresse, Geburts-datum, Geburtsname, -ort und -land, …	Bspw.: Bearbeitung der Nutzeranfragen, Support, …	Bspw.: Löschung erfolgt nach Auflösung des Accounts.
Bspw.: Kontaktdaten	Bspw.: E-Mail-Adressen, Telefonnummern, Fax-nummern, …	Bspw.: Kontaktmöglichkeit mit Nutzern, …	Bspw.: Löschung erfolgt nach Erledigung der Anfrage.
Bspw.: Besonders sensible Daten (Art. 9 DSGVO), insb. Gesundheitsdaten.	Bspw.: Beschäftigtendaten, Sozialdaten, …	Bspw.: Vertragserfüllung , …	Bspw.: Löschung erfolgt nach Vertragserfüllung.
Bspw.: Login-Daten	Bspw.: Benutzername, Passwort, Sicherheitsfrage und -antwort, …	Bspw.: Zur Verifizierung der Nutzer, …	Bspw.: Löschung erfolgt nach Beendigung der Session.
Bspw.: technische Daten	Bspw.: Datum/Uhrzeit (Zeitstempel), IP-Adresse, Cookies, Logfiles, Backups, …	Bspw.: Wartung, Fehleranalyse, technische Optimierung, …	Bspw.: Löschung erfolgt nach 30/60/90 Tagen.
…	…	…	…

Weisungs-/Empfangsberechtigte Personen

Weisungsberechtigte Personen des Verantwortlichen		Zum Empfang von Weisungen berechtigte Personen beim Auftragsverarbeiter	
Name, Vorname	Klicken Sie hier, um Text einzugeben.	Name, Vorname	Klicken Sie hier, um Text einzugeben.
Referat	Klicken Sie hier, um Text einzugeben.	Referat	Klicken Sie hier, um Text einzugeben.
E-Mail	Klicken Sie hier, um Text einzugeben.	E-Mail	Klicken Sie hier, um Text einzugeben.
Telefon	Klicken Sie hier, um Text einzugeben.	Telefon	Klicken Sie hier, um Text einzugeben.

Informationswege

Die Erteilung von Weisungen durch den Verantwortlichen erfolgt schriftlich oder textförmlich (§ 126b BGB) an die zum Empfang von Weisungen berechtigten Personen des Auftragsverarbeiters.
Im Ausnahmefall, zum Beispiel aufgrund einer hohen Dringlichkeit, kann eine Weisung mündlich erteilt werden. Weisungen sind zu dokumentieren.
Im Falle einer mündlich erteilten Weisung bestätigt der Verantwortliche diese dem Auftragsverarbeiter unverzüglich schriftlich oder textförmlich (§ 126b BGB)

Verfahrensspezifische Kontaktdaten

	Eintrag erfolgt durch ITZBund		
	Ansprechpartner/in		Berechtigung in DATSCHA
	Fachverantwortliche/r (AG)	Verfahrensverantwortliche/r (VV)	
Name, Vorname	Klicken Sie hier, um Text einzugeben.	Klicken Sie hier, um Text einzugeben.	VDS
E-Mail	Klicken Sie hier, um Text einzugeben.	Klicken Sie hier, um Text einzugeben.	
Telefon	Klicken Sie hier, um Text einzugeben.	Klicken Sie hier, um Text einzugeben.	

Verfahrensspezifische Netzangaben

Netz								
ITZBund/BFV Netz	NdB (IVBB)	NdB-VN (DOI,Testa)	DEU (Testa-s, CCN/CSI)	BMVI-WAN	IVÖV	AA-Netz	CNP	Sonstiges
☐	☐	☐	☐	☐	☐	☐	☐	Klicken Sie hier, um Text einzugeben.

- **ITZBund-Netz** – Netz der Bundesfinanzverwaltung
- **NdB** (IVBB) – Verbindungsnetz der Ober-/Oberst- und nachgelagerte Bundesbehörden und Bundesverwaltungen
- **NdB-VN** (DOI,Testa) – Verbindungsnetz, Kopplungsnetz Kommunen/Land - Bund
- **DEU** (Testa-s, CCN/CSI) – Europäische Austauschnetze, CCN/CSI (Common Communication Network/Common System Interface) dient insbesondere dem Datenaustausch betreffend verschiedener ZOLL- und Steuerverfahren
- **BMVI-WAN** – Netz der Bundesverwaltung für Verkehr und digitale Infrastruktur
- **IVÖV** – Informationsverbund der öffentlichen Verwaltung
- **AA-Netz** – Netz des Auswärtigen Amtes
- **CNP** – Central Network Police – Netz des Polizeiverbundes

***Die Netzangabe bezieht sich immer auf die speziellere Einheit und den Serverstandort.**

Verfahrensspezifische Betriebsstätten

Berlin	Köln / Bonn	Wiesbaden / Frankfurt	Ilmenau	Nürnberg	Sonstiges
☐	☐	☐	☐	☐	Klicken Sie hier, um Text einzugeben.

Verfahrensspezifische Anforderungen, die nicht durch die Standard-TOM des ITZBund erfüllt werden

Zur Umsetzung der nach § 5 der V-AV genannten Anforderungen sind *verfahrensspezifisch* folgende datenschutzrechtliche Anforderungen für das jeweilige IT-Verfahren zu erheben, die nicht bereits von den Standard-TOM des ITZBund nach *Anlage 3 TOM* abgedeckt sind:

a) <u>Vertraulichkeit</u>
Anforderung zu verfahrensspezifischen Maßnahmen, die bewirken, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können:

……..

……..

……..

……..

b) <u>Integrität</u>
Anforderung zu verfahrensspezifischen Maßnahmen, die bewirken, dass personenbezogene Daten während der Verarbeitung unversehrt und aktuell bleiben:

……..

…….

…….

…….

c) Verfügbarkeit

Anforderung zu verfahrensspezifischen Maßnahmen, die bewirken, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden:

…….

…….

…….

…….

d) Authentizität der Daten

Anforderung zu verfahrensspezifischen Maßnahmen, die bewirken, dass personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können:

…….

…….

…….

…….

e) Revisionsfähigkeit

Anforderung zu verfahrensspezifischen Protokollierungsverfahren, die die Feststellung erlauben, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat:

…….

…….

…….

…….

f) Transparenz

Anforderung zu verfahrensspezifischen Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig und in zumutbarer Zeit nachvollzogen werden können:

…….

……

……

……

Festlegungen der verfahrensspezifischen Datenschutzkonzepte und verfahrensspezifischen Sicherheitskonzepte bezüglich organisatorischer und technischer Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Daten gelten als Bestandteil dieser Vereinbarung.

Subunternehmen

Name der Firma	Postalische Adresse	Im Einsatz für ITZBund seit	Vereinbarte Dienstleistung	V-AV mit ITZBund abge-schlossen am*	Name und Kontaktdaten DSB des Sub.*

Hinweis: Nähere datenschutzrechtliche Konkretisierungen zu den hier aufgelisteten Verfahren finden Sie in der jeweiligen verfahrensspezifischen Anlage zur Leistungsvereinbarung.	
Verfahren xy	**Leistungsbezeichnung/SLA/SVS: AKZ xy**
Verfahren xy	**Leistungsbezeichnung/SLA/SVS: AKZ xy**
…	

Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten nach Art. 32 DSGVO

Verantwortliche/r / Fachauftraggeber/in	Fach-AGS	Klicken Sie hier, um Text einzugeben.
	Name, Vorname	Klicken Sie hier, um Text einzugeben.
	E-Mail	Klicken Sie hier, um Text einzugeben.
	Telefon	Klicken Sie hier, um Text einzugeben.
Datenschutzbeauftragte/r Verantwortliche/r	Name, Vorname	Klicken Sie hier, um Text einzugeben.
	E-Mail	Klicken Sie hier, um Text einzugeben.
	Telefon	Klicken Sie hier, um Text einzugeben.
Datenschutzbeauftragte/r Auftragsverarbeiter/in	Name, Vorname	Köhler, Thomas
	E-Mail	Datenschutzbeauftragte@itzbund.de
	Telefon	+49 228 99680-5018

§ 1 Technische und organisatorische Maßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen in angemessener Form gewährleistet ist. Die Vertragspartner gewährleisten dazu die Umsetzung der in den jeweils relevanten Sicherheitskonzepten für die Verfahren definierten technisch-organisatorischen Maßnahmen.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden die folgenden Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen; sie sind umzusetzen, soweit nicht in den Sicherheitskonzepten bereits anderweitige, mindestens gleichwertige Maßnahmen getroffen worden sind:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	Zutrittskontrolle wird als Gebäudesicherungen in Form von Personenkontrolle durch Pförtner durchgeführt, auch Ausweis- und Chipkartenleser, die nur berechtigten Personen Zutritt gewähren, sind vorhanden. In einzelnen Bereichen wird der Zutritt durch mechanische Schließanlagen mittels Schlüssel gesichert. Zudem wird mithilfe von Alarmanlagen und Schranken eine Einbruchssicherung gewährleistet. Schutzbedürftige Räume sind mit feuerfesten Türen und Sicherheitsschlössern ausgestattet. Beim Verlassen der Räume, werden diese entsprechend mit zugewiesenem Schlüssel oder Chipkarte abgeschlossen. Die Chipkarten sind personalisiert und werden gemeinsam mit den nötigen Schlüsseln bei Dienstantritt den jeweiligen Mitarbeitern ausgehändigt. Die Schlüsselvergabe erfolgt gegen eine Aushändigungsbestätigung und wird entsprechend dokumentiert.
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Der Zugang zu IT-Systemen erfordert zwingend eine Authentisierung des Benutzers nach den Passwort-Richtlinien für das ITZBund, die für alle Beschäftigten beim ITZBund verbindlich sind. Der eingeschränkte Zugang zu den Clients- und Servern erfordert generell eine Identifikation per Benutzername und Passwort der Nutzungsberechtigten (z.B. über eine AD-Authentisierung). Die personalisierte Zugangsberechtigung wird in einem Change-Prozess, in dem Fachverantwortliche und Vorgesetzte beteiligt sind, erteilt. Die Datenkommunikation ist durch mehrstufige Firewall-Systeme, Virtual Private Network (VPN) und Elektronische Signatur, welche dem Stand der Technik entsprechen, abgesichert.

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 nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Grundsätzlich werden nur so viele Zugriffsrechte wie nötig und so wenige wie möglich eingerichtet. Das Rollen- und Berechtigungskonzept des ITZBund regelt, wer Benutzerkennungen beantragen und diese genehmigen darf und welche Kriterien zur Einrichtung berechtigen. Zudem ist festgelegt, wer Benutzer in der Anwendung/im IT-System einrichtet, wie dieses dokumentiert wird und welche Vorgaben/Anforderungen vom Kunden existieren. Berechtigungen werden bei Aufgaben- oder Abteilungswechsel wieder entzogen. Zugriffsberechtigte werden in einem Change-Prozess nach ITIL in einem Datenverarbeitungstool berechtigt, welches auch gleichzeitig die ihnen erteilten Befugnisse dokumentiert. Den Change können wiederum nur Change-berechtigte Personen anstoßen. Die benutzerdefinierten Schreib-, Lese- und Änderungsrechte auf Daten richten sich nach der Zugehörigkeit zu Fach- und Organisationsgruppen sowie nach der Aufgabenwahrnehmung der Person. Über die profilorientierte Zuordnung in Verzeichnisdiensten (AD) und über Berechtigungen auf Dateiservern wird sichergestellt, dass nur Zugriffsberechtige auf die Daten/Dienste zugreifen. Die Benutzerzugriffe werden auf mehreren Instanzen protokolliert und können detailliert nachvollzogen werden. Mehrstufige Firewallsysteme verhindern unberechtigte datenkommunikationsbasierte Zugriffe auf die Systeme. Die Benutzung von USB- und vergleichbaren Schnittstellen mobiler Datenträger ist durch eine zentral verwaltete Schnittstellenkontrollsoftware eingeschränkt. An allen Endgeräten ist nur für die

		dienstlichen Krypto-USB-Sticks die Schnittstelle lesend und schreibend sowie für alle CD/DVD der Lesezugriff freigeschaltet. Nichtmagnetische und hybride elektronische Massenspeicher (SSD-Festplatten, CompactFlash, USB-Sticks etc.) werden bis zur Verfügbarkeit eines BSI-konformen Zerstörungs-/Vernichtungsverfahrens unter Verschluss aufbewahrt. Auftragsverarbeiter und Verantwortlicher stellen im Zusammenwirken die termingerechte, wirksame und nachweisliche Löschung von zu löschenden Daten aus allen Datenbanken, von allen Datenspeichern, Sicherungen und ggf. Archiven sicher.
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.	Der Zutritt zu Räumen und der Zugang zu IT-Systemen (Netzwerkkomponenten, SAN, Datensicherung) erfolgt ausschließlich durch befugte Personen. Die Weitergabekontrolle wird durch entsprechende Serverinstanzen, dedizierte Datenhaltung und verschlüsselte Datenübertragung gewährleistet. Die Schnittstellen zum Internet werden über Content-Proxys und Web-Applikation-Firewallsysteme protokolliert und abgesichert. Die Datenübermittlung via Schnittstellen zwischen den Systemkomponenten des Auftragsverarbeiters und des Verantwortlichen erfolgt ausschließlich über verschlüsselte Verbindungen (HTTPS) und Authentifizierung. In Einzelfällen sind Netzverbindungen mit Kryptotechnik zwischen den Servern Ende-zu-Ende-verschlüsselt. Zwischen dem externen Mailserver des Verantwortlichen und den Mailservern des Auftragsverarbeiters werden E-Mails durch stets aktuell zu haltende Zertifikate automatisch verschlüsselt und signiert ausgetauscht.

		Festplatten mobiler Endgeräte und Telearbeitssysteme und in Einzelfällen bei stationären PC sind verschlüsselt. Rückschlüsse auf Inhalt einzelner Datenträger sind durch Aufdruck gegeben. Der Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden nach § 8 Abs. 1 Satz 1 BSIG wird in allen Fällen des Zugriffs und der Datenübermittlung eingehalten.
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Administrative Zugriffe auf die technischen Systeme werden lokal in systeminternen Logdateien und in betriebssystemeigenen Ereignisprotokollen protokolliert. Darüber hinaus wird über zentrale Logging-Systeme für Firewall und Proxy sichergestellt, dass eine Überprüfung der Zugriffe auf das Grundsystem und nach „Außen“ erfolgt. Die Aufbewahrung nach den Aufbewahrungspflichten gem. § 113 BBG Aufbewahrungsfrist für Log-Dateien und die zentrale Logsysteme wird sichergestellt.
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	Eine ordnungsgemäße Auswahl möglicher Subunternehmen wird auftragnehmerseitig dadurch gewährleistet, dass bereits im Rahmen des Vergabeverfahrens berücksichtigt wird, ob ein potentieller Subunternehmer hinreichende Garantien dafür bietet, dass er eine Verarbeitung personenbezogener Daten entsprechend den Anforderungen der gesetzlichen Datenschutzbestimmungen durchführen wird. Das Auftragsverarbeitungsverhältnis zwischen Auftragsverarbeiter und Subunternehmen wird durch einen schriftlichen Vertrag nach Art. 28 Abs. 4 DSGVO i.V.m. Art. 28 Abs. 3, 9 DSGVO geregelt. Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n bestellt.

7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Die Objektsicherungsmaßnahmen im Katastrophen- oder Notfallplan, sowie die Schwachstellenanalyse und die sichere Versorgung der Rechenzentren werden im Sicherheitskonzept geregelt. Alle Netzkomponenten (Switche, Firewallsysteme, Stromversorgung) und IT-Systeme (Server, NAS, VMs) werden auf Anomalien sowie auf Verfügbarkeit überwacht. Die Daten werden durch redundante Hochleistungsspeichersysteme, automatisierte regelmäßige Sicherungen sowie Archivierung vor Zerstörung/Verlust geschützt. Redundant aufgestellte IT-Systeme in dedizierten Räumen, gespiegelte Festplatten und der Einsatz von unterbrechungsfreien Stromversorgungen stellen sicher, dass Daten nicht verloren gehen. Supportverträge zwischen dem IT-Dienstleister des ITZBund und den Herstellern der eingesetzten Produkte stellen die Aufrechterhaltung und Wartung der technischen Systeme für die Auftragsverarbeitung sicher.
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Mandantentrennung wird mittels Kennzeichnung der Daten unterschiedlicher Verantwortlicher softwareseitig gewährleistet. Bei Bedarf wird für die Serversysteme und Netzkomponenten die stärkste Form der Mandantentrennung vorgenommen und die Daten damit vollständig von anderen Aufgabenbereichen des Auftragnehmers getrennt. Weiterhin werden Test- und Produktivsystemen getrennt und auf unterschiedliche Datenbasen zugegriffen. Die durch die Anbindung von externen Netzwerken mit unterschiedlichem Schutzniveau (Internet, IVBB/NdB, Hausnetze) begründeten Anforderungen sind in der System-, Anwendungs- und Sicherheitsarchitektur berücksichtigt.

(2) Es ist im Rahmen des Datenschutzmanagements ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.