Vereinbarung zur Auftragsverarbeitung

als
Anlage 4
zum
EVB-IT Systemvertrag
über den Systembetrieb der Digitalen Einreiseanmeldung (DEA)

- nachfolgend „**Leistungsvereinbarung**" -

zwischen der

Bundesrepublik Deutschland
vertreten durch das Robert Koch-Institut
Nordufer 20
13353 Berlin

- nachfolgend „**Verantwortlicher**" -

und der

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin

- nachfolgend „**Auftragsverarbeiter**" -

- beide nachfolgend gemeinsam „**Vertragsparteien**" -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

Die papierbasierte Aussteigekarte soll durch eine volldigitale Lösung ersetzt werden. Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat dafür mit seinem Projekt „Digitale Einreiseanmeldung" (DEA) im Auftrag des Bundesministeriums für Gesundheit (BMG) eine technische Lösung durch den Auftragsverarbeiter entwickeln lassen. Nach fachlicher Vorgabe wird die digitale Einreiseanmeldung die zuständigen Stellen in der Überwachung der jeweils geltenden Quarantäneverordnung unterstützen.

In der volldigitalen Lösung erfassen die Reisenden ihre Daten in einem Web-Formular, das gleichermaßen auf Smartphones und Desktop-PCs funktioniert, barrierefrei und auf vollständiges Befüllen („Konversion") optimiert ist. Das Web-Formular basiert im Wesentlichen auf der Papier-Aussteigekarte und den fachlichen Anforderungen zur Erfassung der Reisenden.

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, haben die Vertragsparteien einen Auftragsverarbeitungsvertrag abgeschlossen. Seitdem wurde der Leistungsinhalt weiterentwickelt und der Umfang der Auftragsverarbeitung angepasst. In Bezug auf diese Entwicklungen schließen die Vertragsparteien die nachfolgende Vereinbarung. Diese Vereinbarung ändert alle vorherigen Vereinbarungen zwischen den Vertragsparteien über die Auftragsverarbeitung im Rahmen von DEA und geht diesen vor.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Verarbeitung aller personenbezogener Daten (im Folgenden: Daten) im Sinne von Art. 4 Nr. 1, 2 DSGVO, die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung erhoben 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 Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung stellen sich wie folgt dar:

Für den Flug- und Schiffsverkehr sowie den grenzüberschreitenden Bus- und Bahnverkehr aus Covid19-Risikogebieten im Ausland (nachfolgend „Risikogebiete" genannt) wurden Aussteigekarten angeordnet. Die papierbasierte Aussteigekarte soll durch eine digitale Lösung ergänzt bzw. ersetzt werden. Das hier gegenständliche digitale Verfahren bildet funktional ein Äquivalent zum analogen Prozess mit dem Ziel, dass die erhobenen Daten schneller, zielgerichteter und in einem einheitlichen Format derjenigen Behörde zur Verfügung gestellt werden können, die für die Kontrolle der Einhaltung der Quarantänepflicht sowie der Voraussetzungen der landesrechtlichen Ausnahme von der Quarantänepflicht zuständig ist, etwa das Gesundheitsamt oder die Polizeibehörde (nachfolgend „zuständige Behörde" genannt).

Für die zentrale Übermittlung der Datensätze an die zuständigen Behörden, die nach erfolgter Übermittlung dann das dortige Verwaltungsverfahren eröffnen, gibt es zwei unterschiedliche Varianten. Die erste Variante, die eine VPN-TLS-basierte sichere Anbindung der zuständigen Behörden an das von dem Auftragsverarbeiter zur Verfügung gestellte System erfordert, wird nachfolgend unter lit. a) dargestellt. Als zweite Variante werden die Daten über eine Clearing-Stelle direkt an den Verantwortlichen übermittelt, wie nachfolgend unter lit. b) dargestellt.

a) Direkte Anbindung der zuständigen Behörden [redacted]
Der Einreisende ruft für die Dateneingabe eine Webseite über seinen PC oder sein Smartphone auf. Dabei werden die unter § 2 (2) a) aufgeführten Daten erhoben, um die Webseite bereitzustellen. Die Verbindung ist dabei über [redacted] – abgesichert.

Nach Aufruf der Webadresse wird durch Eingabe des relevanten Landes oder Gebietes geprüft, ob es sich um ein Risiko-, Virusvarianten- oder Hochinzidenzgebiet (nachfolgend „Risikogebiet" genannt) handelt. Nach der Prüfung des Risikogebiets erscheint eine Meldung auf der Webseite, die dem Einreisenden entweder die Pflicht zur Übermittlung der Reiseangaben und persönlichen Daten sowie ggfs. eine Testpflicht vor Reiseantritt bzw. nach Einreise anzeigt oder aber mitteilt, dass eine entsprechende Übermittlung an die zuständige Behörde nicht erforderlich ist. Nur in ersterem Fall erscheint der Button „zur Eingabe", wonach der Einreisende auf die eigentliche Dateneingabeseite weitergeleitet wird.

Nach Eingabe der Daten wird dem Einreisenden eine PDF-Datei angezeigt, die dieser als Nachweis der Datenübermittlung herunterladen kann. Die PDF-Datei enthält einen Link, unter dem der Einreisende die Kopie eines negativen Testergebnisses bzw. eines Genesenen- oder Impfnachweises (im Folgenden: Nachweis) hochladen kann. Für das Hochladen des Nachweises erhält der Reisende zudem eine PIN an seine E-Mail-Adresse oder persönliche Mobilnummer, die genutzt werden muss, um die Kopie des Nachweises hochladen zu können.
Technisch erfolgt die Eingabe der Daten bzw. der Kopie des Nachweises wie folgt:

- Die Eingabe des Einreisenden – also die Auswahl des relevanten Landes, die folgende Eingabe der Daten sowie der Kopie des Nachweises – erfolgt auf dem lokalen Gerät des Einreisenden.
- Die Verschlüsselung der Digitalen Einreise-Anmelde-Daten (einschließlich der Kopie des Nachweises) [redacted]
§ 6 IFG
[redacted]

Nach Übermittlung der verschlüsselten Datensätze von den lokalen Geräten der Einreisenden an den Server des Auftragsverarbeiters wird dort eine Sortierung der Datensätze nach Postleitzahl vorgenommen. Die Datensätze werden dann den zuständigen Gesundheitsämtern zur Verfügung gestellt. Die hochgeladene Kopie des Nachweises wird der Einreiseanmeldung des Einreisenden zugeordnet.

Die zuständigen Behörden haben nur Zugriff auf den Teil der gespeicherten Einreiseanmeldungen, der innerhalb ihres örtlichen Zuständigkeitsbereiches liegt. Die zuständige Behörde wird anhand der Postleitzahl des Zielortes ermittelt. Mit einem spezifischen öffentlichen Schlüssel der zuständigen Behörde wird das Datenpaket so übermittelt, dass nur diejenige zuständige Behörde die Datensätze entschlüsseln kann, die über den passenden Schlüssel verfügt.

b) Übermittlung durch Verantwortlichen

Alle PLZ, welche im Frontend des Reisenden keiner zuständigen Behörde zugeordnet werden können und für die somit kein öffentlicher Schlüssel zur Verschlüsselung zur Verfügung steht, werden mit dem öffentlichen S[redacted]l des Verantwortlichen verschlüsselt. Der Verantwortliche greift über einen [redacted] auf den Web-Zugriff zu und kann dort alle nicht zugewiesenen Datensätze vorfinden. Der Verantwortliche ist nun in der Lage, anhand der detaillierten Merkmale über die PLZ hinaus eine eindeutige Zuweisung an eine zuständige Behörde vorzunehmen. Für diese Einzelfälle kann die Clearing-Stelle des Verantwortlichen derzeit einen CSV-Export generieren, welchen er über einen gesicherten Austausch mittels [redacted]

(2) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

a) Daten aller Reisenden und sonstiger Webseitenbesucher,

- IP-Adresse
- Datum und Uhrzeit der Anfrage
- Zeitzonendifferenz zur Greenwich-Mean-Time (GMT)
- Inhalt der Anforderung (konkrete Seite)
- Zugriffsstatus / HTTP-Statuscode
- jeweils übertragene Datenmenge
- Webseite, von der die Anforderung kommt
- Browser
- Betriebssystem und dessen Oberfläche
- Sprache und Version der Browsersoftware

b) Reisedaten des Reisenden aus einem Risikogebiet, je nach Reisemittel

aa) Flugzeug

- Flugnummer
- Name der Fluggesellschaft

- Abflugort
- Sitzplatz
- Einreisedatum
- Umstieg

bb) Bahn

- Zugnummer
- Anbieter
- Abfahrtsort
- Sitzplatz oder Wagennummer
- Einreisedatum
- Umstieg

cc) Bus

- Name des Busunternehmens
- Liniennummer
- Abfahrtsort
- Sitzplatz
- Einreisedatum

dd) Auto

- Abfahrtsort
- Einreisedatum

ee) LKW

- Unternehmensname
- Abfahrtsort
- Einreisedatum

ff) Schiff

- Schiffsname
- Nummer der Schifffahrt
- Letzter Hafen
- Einreisedatum
- Kabinennummer

ff) Andere

- Abreiseort
- Einreisedatum

c) Stammdaten und besuchte Länder des Reisenden aus einem Risikogebiet

- Nachname (Familienname)
- Vorname
- Geschlecht (weiblich/männlich/divers)
- Geburtstag
- Ausweisnummer
- Persönliche Telefonnummer
- Weitere Telefonnummer
- E-Mail-Adresse
- Länder, in denen sich der Einreisende in den letzten 10 Tagen aufgehalten hat, sowie Einordnung der Länder als Risiko-, Virusvarianten- oder Hochinzidenzgebiet

d) Anschrift des Reisenden aus einem Risikogebiet für den anschließenden Quarantänezeitraum

- Beherbergungsbetrieb

- Straße
- Hausnummer
- Wohnungsnummer
- Postleitzahl oder Stadt
- Bundesland

e) Angaben, ob ein Impf-, Test- oder Genesenennachweis („Nachweis") vorliegt, und ob typische Symptome für eine Infektion mit dem Coronavirus SARS-CoV-2 vorliegen;

f) Optional kann der Reisende aus einem Risikogebiet noch (i) eine weitere Anschrift hinzufügen, sollte diese für den Zeitraum der nächsten 10 Tage für eine Kontrolle der Einhaltung der Quarantänevorschriften relevant sein, (ii) einen auf den Reisenden zutreffenden Ausnahmetatbestand von der Anmelde-, Quarantäne- und / oder Nachweispflicht oder (iii) die Kopie eines Nachweises hochladen.

g) Dienstliche E-Mail-Adresse und individuelles Passwort der mit der DEA befassten Beschäftigten der zuständigen Behörden.

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist Folgender:

- Besucher des Web-Formulars,
- die Reisenden aus Risikogebieten,
- Beschäftigte der zuständigen Behörden.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) 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.

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

(3) Soweit sich ein Reisender zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) 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 definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften der Europäischen Union oder der Mitgliedstaaten. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen schriftlich 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 folgende:

Weisungsberechtigte Person auf Seiten des Verantwortlichen:

§ 5 Abs. 1 IFG [redacted]

Zum Empfang von Weisungen berechtigte Person auf Seiten des Auftragsverarbeiters:

§ 5 Abs. 1 IFG [redacted]

(6) 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.

(7) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Verfügung, die der Verantwortliche für das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30. Abs. 1 DSGVO benötigt. 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.

(8) § 6 IFG [redacted]

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) 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.

(2) 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.

(3) 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.

(4) 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

(1) Die Vertragsparteien vereinbaren die in dem **Anhang 1** „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem **Anhang 1** „Technisch-organisatorische Maßnahmen" festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) 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 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche oder ein anderer von diesem beauftragter Dritter 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. Der Verantwortliche darf als Dritten im Sinne der Absätze 4 und 5 nur eine in Deutschland anerkannte Wirtschaftsprüfungsgesellschaft auf eigene Kosten einsetzen. Der Dritte ist im Vorhinein schriftlich zur Geheimhaltung und zur Einhaltung der IT- und Informationssicherheitsvorgaben des Auftragsverarbeiters zu verpflichten. Die ordnungsgemäße Verpflichtung weist der Verantwortliche dem Auftragsverarbeiter auf Anforderung unverzüglich nach.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen oder einem anderen von diesem beauftragten Dritten darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4, für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) und ggfs. für eine vorherige Konsultation mit der Aufsichtsbehörde (Art. 36 DSGVO) benötigt.

(6) 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 Betroffene 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

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

(2) 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.

(3) 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 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Unterauftragnehmer) nur mit vorheriger ausdrücklicher schriftlicher Genehmigung des Verantwortlichen in Anspruch nehmen. Der Auftragsverarbeiter setzt zum Zeitpunkt des Vertragsschlusses die im Anhang 2 benannten Subunternehmen zur Erfüllung seiner Pflichten ein. Beabsichtigt der Auftragsverarbeiter, zur Erfüllung dieses Vertrages zu einem auf den Vertragsschluss folgenden Zeitpunkt weitere Subunternehmen einzusetzen oder bereits eingesetzte Subunternehmer auszuwechseln, sind diese ebenso in **Anhang 2** „Liste von beauftragten Subunternehmern" zu bezeichnen.

(2) 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.

(3) 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.

(4) Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die aufgrund dieser Vereinbarung ihm gegenüber geltenden Regeln auch in seinem Verhältnis zum Subunternehmer gelten. Die Vertragsparteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag zwischen Auftragsverarbeiter und Subunternehmer ein dieser Vereinbarung entsprechendes Schutzniveau aufweist bzw. dem Subunternehmer die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche 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.

(5) 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 Datenschutzbeauftragten des Verantwortlichen oder einem von diesem beauftragten Dritten 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 oder einem von diesem beauftragten Dritten 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.

§ 5 Abs. 4 Satz 2 findet auf den vom Verantwortlichen beauftragten Dritten Anwendung.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage 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.

(2) 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.

§ 5 Abs. 1 IFG