Vereinbarung zur Auftragsverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [*Datum*]
- nachfolgend „Leistungsvereinbarung“ -

zwischen der
Bundesrepublik Deutschland, vertreten durch das

Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit,
dieses vertreten durch das

Bundesamt für Naturschutz, Konstantinstraße 110, 53179 Bonn
- nachfolgend „Verantwortlicher“ -

und

[*Vertragspartner*]

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

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

(1) Die Vereinbarung findet Anwendung auf die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen und auf Weisung des Verantwortlichen verarbeitet werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

(2) Dieser Vertrag gilt vorranging vor anderen Vereinbarungen und Abreden zwischen Auftraggeber und Auftragnehmer, es sie denn, zwischen den Parteien wird ausdrücklich etwas anderes vereinbart.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung, die dieser Vereinbarung angefügt ist.

(2) In der Anlage „Betroffene Personen, Datenarten und Kategorien“ werden die Daten, die Gegenstand dieser Vereinbarung sind, konkret benannt.

§ 3 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die Ihnen durch die Datenschutzgesetze (insb. DSGVO) auferlegten Pflichten einzuhalten. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

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

(3) Soweit sich eine betroffene Person 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 Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(7) Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher (oder dokumentierter elektronischer) Zustimmung durch den Verantwortlichen erteilen, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet.

(8) Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(9) 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.

(10) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet *der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR) / der Bundesrepublik Deutschland* statt. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage schriftlicher (oder dokumentierter elektronischer) Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(11) Der Auftragsverarbeiter gewährleistet, 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 (oder dokumentierten elektronischen) Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen (Anhang „Home Office, Mobiles Arbeiten“) für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter gewährleistet, 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) Sofern der Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragte/n unterliegt sind die Kontaktdaten der/des Datenschutzbeauftragten dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen. Unterliegt der Auftragsverarbeiter nicht der Benennungspflicht, teilt er dem Verantwortlichen die Kontaktdaten eines Ansprechpartners für den Datenschutz mit.

(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 „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang „Technisch-organisatorische Maßnahmen“ ist Gegenstand dieser Vereinbarung.

(2) Ergibt eine vom Verantwortlichen durchzuführende Prüfung einen Anpassungsbedarf hinsichtlich der vom Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen, sind die Anpassungen im Einvernehmen zwischen beiden Parteien umzusetzen.

(3) 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 „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) 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.

(5) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, 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 erfolgen. 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.

(6) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Der Verantwortliche kann sich hierzu 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.

(7) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(8) 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 im Auftrag des Verantwortlichen verarbeitete personenbezogene Daten dem Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. 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 keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß dieser Vereinbarung durchführt, ohne vorherige gesonderte schriftliche (oder dokumentierte elektronische) Genehmigung des Verantwortlichen an einen

Subunternehmer untervergeben. Der Auftragsverarbeiter reicht den Antrag für die gesonderte Genehmigung mindestens vier Wochen vor der Beauftragung des betreffenden Subunternehmers zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Subunternehmer findet sich im Anhang „Subunternehmen“. Die Parteien halten den Anhang jeweils auf dem neuesten Stand.

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.

(2) 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.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche (oder dokumentierte elektronische) 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.

(4) 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 zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit dem/ der Datenschutzbeauftragten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Haftung und Schadenersatz

Auf Artikel 82 DSGVO wird bezüglich der Haftung und des Rechts auf Schadenersatz verwiesen.

§ 11 Schlussbestimmungen

(1) 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.

(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.

Datum, Ort	Datum, Ort
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Weisungsbefugnis" zu § 3 (nach Zuschlagserteilung auszufüllen, optional)

zur Vereinbarung zur Auftragsverarbeitung vom [Datum]
zwischen der Bundesrepublik Deutschland, vertreten durch das Bundesamt für Naturschutz

und [Vertragspartner]

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 nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Verantwortlichen:
Seitens des BfN sind alle Personen des BfN gegenüber dem Auftragnehmer grundsätzlich Weisungsbefugt.

Zum Empfang der Weisungen berechtigte Personen auf Seiten des Auftragsverarbeiters:

- *Y (für … Bereich)*
- *YY (für … Bereich)*
- *YYY (Stellvertreter)*
- …

Vorgesehene Informationswege, wenn Weisung nach Meinung des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt:
[Zutreffendes bitte ankreuzen]

X schriftliche und/oder

X elektronische und/oder

☐ mündliche Information

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren. Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Anhang „Technisch-organisatorische Maßnahmen (TOM)"

zur Vereinbarung zur Auftragsverarbeitung vom [*Datum*]
zwischen der Bundesrepublik Deutschland, vertreten durch das Bundesamt für Naturschutz
und [*Vertragspartner*]

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
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 Person in angemessener Form gewährleistet ist.

§ 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 folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 5 DSGVO dienen:

a) Transparenz

Transparenz im Sinne des Art. 5 Abs. 1 lit. a DSGVO ist gewährleistet, wenn die Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

- ☐ Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- ☐ Dokumentation der Datenempfänger und Zeitspanne der Überlassung
- ☐ Dokumentation der Mandanten und zugehörigen Datenbereiche
- ☐ Dokumentation verbindlicher Löschfristen
- ☐ Dokumentation von Auftrags- und Unterauftragsverhältnissen
- ☐ Veröffentlichung der Dokumentationen (z. B. online)
- ☐ Bereitstellung der hier markierten Dokumentationen auf Antrag der betroffenen Person
- ☐ Veröffentlichung der Informationen zur Verarbeitung von personenbezogenen Daten (z. B. online oder als Aushang) als Datenschutzerklärung
- ☐ _____

b) Zweckbindung

Zweckbindung im Sinne des Art. 5 Abs. 1 lit. b DSGVO ist gewährleistet, wenn die Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- ☐ Darstellung der Zwecke im Verzeichnis von Verarbeitungstätigkeit
- ☐ Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DS-GVO
- ☐ Erlass einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten
- ☐ Entgegennehmen ausschließlich schriftlicher Weisungen nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers
- ☐ _____

☐

c) Datenminimierung

Datenminimierung im Sinne des Art. 5 Abs. 1 lit. c DSGVO ist gewährleistet, wenn die Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind.

☐ Datenschutz durch Technikgestaltung (data protection by design)
☐ Vornahme datenschutzfreundlicher Voreinstellungen (data protection by default)
☐ Plausibilitätskontrollen zur Beschränkung der Datenerhebung
☐ Festlegung verbindlicher Löschfristen
☐ Festlegung automatisierter Löschzyklen
☐ Regelmäßiges manuelles Auslösen der Löschung nicht benötigter Daten.
☐ Pseudonymisierung der Daten bei Weiterverarbeitung oder Übermittlung
☐ Anonymisierung von Daten wenn Identifikation nicht mehr notwendig
☐ Regelmäßige Audits über den Datenumfang (durch Datenschutzbeauftragte)
☐ _____

d) Richtigkeit

Richtigkeit im Sinne des Art. 5 Abs. 1 lit. d DSGVO ist gewährleistet, wenn die verarbeiteten Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind und Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

☐ Nachweis der Herkunft von Daten
☐ Zertifikatsbasierte Authentifizierung der Datenquelle
☐ Identitätsprüfung bei Anlieferung von Daten
☐ Nutzung des Post-Ident-Verfahrens
☐ Nutzung eines Video-Ident-Verfahrens
☐ Unverzügliche Löschung unrichtiger Daten
☐ Unverzügliche Berichtigung unrichtiger Daten
☐ Beantragung einer Berichtigung durch elektronische Antragstellung
☐ Einrichtung eines Verfahrens zur Berichtigung von Daten auf Antrag
☐ Eigenständige elektronische Berichtigung der Daten durch die betroffene Person
☐ _____

e) Speicherbegrenzung

Speicherbegrenzung im Sinne des Art. 5 Abs. 1 lit. e DSGVO ist gewährleistet, wenn die verarbeiteten Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

☐ Frühzeitige Anonymisierung personenbezogener Daten
☐ Frühzeitige Pseudonymisierung personenbezogener Daten
☐ _____

(2) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

a) Vertraulichkeit

Vertraulichkeit im Sinne des Art. 32 Abs 1 lit. b in Verbindung mit ErwGr 39 und 83 DSGVO ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können und die Daten außerdem gemäß Art. 5 Abs. 1 lit. f DS-GVO vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind.

- ☐ Alarmanlage
- ☐ Wachpersonal
- ☐ Zugangskontrollsystem
- ☐ Unterteilung in Sicherheitszonen
- ☐ Sicherheitsschlösser
- ☐ Schlüsselregelung
- ☐ Schließsystem mit Chipkarte / Transponder / Codesperre / manuell
- ☐ Biometrische Zugangssperren
- ☐ Ausweispflicht
- ☐ Personenkontrolle
- ☐ Festlegung befugter Personen
- ☐ Einbruchhemmende Fenster und Türen
- ☐ Geräte- und Gehäuseversiegelung
- ☐ Auf Datenschutz verpflichtetes Reinigungspersonal
- ☐ Auf Datenschutz verpflichtetes Wartungspersonal
- ☐ Festgelegte Reinigungszeiten
- ☐ Beaufsichtigung von Wartungstätigkeiten
- ☐ Zugangsbeschränkung nach Endgerät
- ☐ Zeitliche Zugangsbeschränkung
- ☐ Benutzerkonto für jeden Mitarbeiter
- ☐ Implementierung eines Rollen- und Berechtigungskonzepts
- ☐ Arbeiten mit individuellen Benutzerkennungen
- ☐ Dem Zweck angemessene Passwort-richtlinien
- ☐ Authentifikation mit SmartCard
- ☐ Biometrische Authentifikation
- ☐ Regelungen beim Ausscheiden von Mitarbeitern
- ☐ Sperren der Bootkonfiguration (BIOS, UEFI)
- ☐ Automatische Abmeldevorgänge
- ☐ Kontensperrung nach mehrmaliger Falscheingabe des Passworts
- ☐ Vergabe von Administratorrechten an minimale Anzahl Personen
- ☐ Sicheres Löschen von Datenträgern / einzelner Dateien
- ☐ Differenzierung administrativer Aufgaben
- ☐ Dateiverschlüsselung
- ☐ Datenträgerverschlüsselung
- ☐ Verschlüsselung von Datenbanken
- ☐ Sperrung der Nutzung von persönlichem Cloud-Speicher am Arbeitsplatz-PC
- ☐ Verhinderung nicht-autorisierter Cloud-Synchronisation durch Drittanbietersoftware
- ☐ Übermittlung von Daten in anonymisierter Form
- ☐ Übermittlung von Daten in pseudonymisierter Form
- ☐ Sichere Behältnisse bei physischem Transport
- ☐ Zuverlässiges Transportpersonal
- ☐ Identitätsnachweis des Transportpersonals
- ☐ Datenträgervernichtung nach DIN 66399
- ☐ Nach Verarbeitungszweck differenziertes Berechtigungskonzept
- ☐ Logische Mandantentrennung
- ☐ Physikalisch getrennte Speicherung und Verarbeitung
- ☐ Trennung von Produktiv- und Testsystem

- ☐ Fernlöschung von mobilen Endgeräten
- ☐ E-Mail-Verschlüsselung mit S/MIME
- ☐ E-Mail-Verschlüsselung mit OpenPGP
- ☐ Durchgängige Transportverschlüsselung bei der E-Mail-Übertragung
- ☐ Transportverschlüsselte Datenübertragung
- ☐ Datenkommunikation über VPN-Tunnel
- ☐ _____

b) Integrität

Integrität im Sinne des Art. 32 Abs 1 lit. b in Verbindung mit Art. 5 Abs. 1 lit. f DSGVO ist gewährleistet, wenn Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt sind.

- ☐ Signieren elektronischer Dokumente
- ☐ Signieren von E-Mails
- ☐ Anwendung von Prüfsummenverfahren
- ☐ Überwachung von Fernwartungsaktivitäten
- ☐ Sperren externer Schnittstellen wie USB
- ☐ Intrusion Detection System
- ☐ Einsatz von Virenschutzlösungen
- ☐ Application Layer Firewall
- ☐ E-Mail-Signierung mit S/MIME
- ☐ E-Mail-Signierung mit OpenPGP
- ☐ Verschlüsselung der Internetpräsenz
- ☐ Packet Filter Firewall
- ☐ Dedizierte Netze für Systeme mit sensiblen Daten
- ☐ Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste
- ☐ Differenzierte Berechtigungen für unterschiedliche Transaktionen
- ☐ Differenzierte Berechtigungen für Datenobjekte
- ☐ Plausibilitätskontrollen bei der Datenverarbeitung
- ☐ Inhaltsverschlüsselte Datenübertragung
- ☐ Regelung zum Umgang mit mobilen Datenträgern
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ E-Mail-Gateway mit Filterfunktion
- ☐ _____

c) Verfügbarkeit

Verfügbarkeit im Sinne des Art. 32 Abs. 1 lit. b DSGVO ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss gemäß Art. 32 Abs. 1 lit. c DSGVO die Fähigkeit existieren die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können.

- ☐ Sicherungs- und Wiederherstellungskonzept (Backup & Recovery)
- ☐ Automatisiertes Anfertigen von Datensicherungen (Backup)
- ☐ Aufbewahrung von Datenträgern in gegen Elementarschäden gesicherten Behältnissen
- ☐ Aufbewahrung der Datensicherung in einem anderen Brandabschnitt
- ☐ Festgelegte Zuständigkeiten für die Datensicherung
- ☐ Regelmäßiger Test der Datenwiederherstellung
- ☐ Notfallplan zur Wiederinbetriebnahme von Servern und Diensten
- ☐ Datenträgerspiegelung (RAID)

- ☐ Datenreplikation
- ☐ Vermeidung lokaler Datenspeicherung
- ☐ Notfallplan bei Kompromittierung
- ☐ Notfallplan bei Datenverlust
- ☐ Redundante IT-Systeme
- ☐ Virtualisierte Infrastruktur
- ☐ Automatisches Benachrichtigungssystem bei Ausfall
- ☐ _____

d) Belastbarkeit

Belastbarkeit ist gemäß Art. 32 Abs. 1 lit. b DSGVO auf Dauer sicherzustellen und betrifft Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

- ☐ Lastausgleich (load balancing) der Netzwerkkomponenten /Server / Dienste
- ☐ Automatische Skalierung virtueller Systeme
- ☐ Unterbrechungsfreie Stromversorgung
- ☐ Überspannungsschutz
- ☐ Klimaanlage in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen
- ☐ Feuerlöscher / automatisches Löschsystem
- ☐ Automatisches Benachrichtigungssystem bei Erreichung der max. Auslastung
- ☐ IT-Komponenten verfügen über erforderliche Leistungsfähigkeit
- ☐ Schutz vor Wassereinbruch
- ☐ Schutz vor Hochwasser
- ☐ Automatisches Notrufsystem
- ☐ Eignung der Räumlichkeiten / des Baus
- ☐ _____

(3) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Rechenschaftspflicht im Sinne des Art. 5 Abs. DSGVO und Wirksamkeitsnachweis im Sinne des Art. 32 Abs. 1 lit. d DSGVO dienen:

a) Rechenschaftspflicht

Rechenschaftspflicht im Sinne des Art. 5 Abs. 2 DSGVO ist erfüllt, wenn der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen kann.

b) Wirksamkeitsnachweis

Gemäß Art. 32 Abs. 1 lit. d DSGVO muss der Verantwortliche in der Lage sein, die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüfen, bewerten und evaluieren zu können. Außerdem muss er gem. ErwGr 87 DSGVO sofort feststellen können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.

- ☐ Führen eines Verzeichnisses von Verarbeitungstätigkeiten
- ☐ Bestellung eine(r/s) Datenschutzbeauftragten
- ☐ Dokumentation über vorhandene IT-Infrastruktur

- ☐ Dokumentation über eingesetzte Programme und Anwendungen
- ☐ Dokumentation der getroffenen Sicherheitsmaßnahmen (im Verzeichnis von Verarbeitungstätigkeiten)
- ☐ Dokumentation der Vernichtung oder Rückgabe von Datenträgern und Unterlagen nach Beendigung eines Auftrags
- ☐ Protokollierung der Anmeldevorgänge
- ☐ Protokollierung der Datenzugriffe
- ☐ Protokollierung gescheiterter Zugriffsversuche
- ☐ Sicherung der Protokolldaten gegen Veränderung und Verlust
- ☐ Automatisierte Auswertung der Protokolldaten
- ☐ Protokollierung der Datenträgervernichtung
- ☐ Protokollierung von Löschvorgängen
- ☐ Protokollierung der Übermittlungsvorgänge
- ☐ Videoüberwachung bei Zutritt zur Datenverarbeitungsanlage
- ☐ Benutzerkennungsbezogene Protokollierung
- ☐ Dokumentation der Übergabeprozesse bei physischem Transport von Datenträgern
- ☐ Protokollierung des Zutritts zu Datenverarbeitungsanlagen oder Räumen in denen Datenverarbeitung stattfindet
- ☐ Protokollierung aller Administratorenaktivitäten
- ☐ Protokollierung der Eingabe bei der Erhebung und Ergänzung von Daten
- ☐ Protokollierung der Veränderung oder Korrektur von gespeicherten Daten
- ☐ Protokollierung der sicheren Löschungen von Datenträgern
- ☐ Stichprobenartige Überprüfung der Wirksamkeit bestimmter Maßnahmen
- ☐ _____

(4) Es ist 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.

(5) Folgende Nachweise werden dieser Vereinbarung angefügt: [Zutreffendes bitte ankreuzen]

- ☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
- ☐ Zertifizierung nach Artikel 42 DSGVO
- ☐ Prüfberichte, Testate etc. unabhängiger Prüfer, bspw. Wirtschaftsprüfer, Auditoren, Datenschutzbeauftragte etc.
- ☐ geeignete Zertifizierung durch einen Auditprozess

(2) Es ist 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.

(3) Folgende Nachweise werden dieser Vereinbarung angefügt: [Zutreffendes bitte ankreuzen]

- ☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
- ☐ Zertifizierung nach Artikel 42 DSGVO
- ☐ Prüfberichte, Testate etc. unabhängiger Prüfer, bspw. Wirtschaftsprüfer, Auditoren, Datenschutzbeauftragte etc.
- ☐ geeignete Zertifizierung durch einen Auditprozess

Anhang „Subunternehmen" zu § 8

Nach § 8 Abs. 1 S. 2 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Gem. § 8 Abs. 1 S. 3 der Vereinbarung erklärt sich der Verantwortliche mit deren Beauftragung einverstanden.

Subunternehmen (Name, Anschrift bzw. Sitz)	Datum des Abschlusses der Vereinbarung zur Auftragsverarbeitung	(Teil-)Leistungsgegenstand im Rahmen der Auftragsverarbeitung

Anhang „Home Office, Mobiles Arbeiten" zu § 3 Abs. 11

Seitens des Auftragnehmers wurden Regelungen getroffen:

- □ unter welchen Arbeitsplatzbedingungen schützenswerte Informationen verarbeitet werden dürfen
- □ wie Daten vor ungewollter Einsichtnahme Dritter zu schützen sind
- □ welche Arbeitsumgebungen komplett verboten sind
- □ welche Informationen außerhalb der Institution transportiert werden dürfen
- □ welche Schutzvorkehrungen beim Transport zu treffen sind
- □ unter welchen Rahmenbedingungen mit mobilen IT-Systemen auf interne Informationen der Institution zugegriffen werden darf
- □ welche Arten von Informationen auf mobilen IT-Systemen verarbeitet werden dürfen
- □ wie sichergestellt wird, dass Unbefugte zu keiner Zeit Zugriff auf dienstliche IT bekommen (z.B. Sperren des Arbeitsplatzes beim Verlassen, Entsperren nach Authentifizierung)
- □ wie sichergestellt wird, dass Unbefugte zu keiner Zeit Zugriff auf dienstliche Unterlagen bekommen
- □ ob und wie fremde IT-Systeme verwendet werden dürfen (BYOD)
- □ zur Meldung bei Verlust von IT oder Unterlagen
- □ zur Entsorgung vertraulicher Informationen und Datenträger
- □ zur regelmäßigen Schulung und Sensibilisierung bezüglich der besonderen Gefahren
- □ zur Verschlüsselung tragbarer IT-Systeme und Datenträger
- □ Sichtschutz zu verwenden ist.
- □ zu Kriterien zur Festlegung der Arbeitsumgebung

Alle für die Mitarbeitenden geltenden Sicherheitsanforderungen für mobile Arbeitsplätze sind dokumentiert und sind für die Mitarbeitenden verpflichtend.

Anhang „Betroffene Personen, Datenarten und Kategorien" zu § 2

Art der Auftragsverarbeitung

- ☐ Organisation einer Konferenz/Workshop/Veranstaltung vor Ort / virtuell / hybrid
- ☐ Erstellung eines Druckwerkes zur Veröffentlichung
- ☐ Bereitstellung einer Softwareanwendung (Software as a service)
- ☐ IT-Dienstleistungen für das BfN
- ☐ _____

Kreis der durch den Umgang mit ihren Daten betroffenen Personen

- ☐ potentielle ☐ Konferenz-/ Workshop- /Veranstaltungsteilnehmende
- ☐ potentielle ☐ Vortragende
- ☐ Fachpublikum
- ☐ Anwohnende
- ☐ Flächenbesitzende
- ☐ BfN-Mitarbeitende
- ☐ Softwarenutzende
- ☐ Antragsteller
- ☐ Interessenten
- ☐ Projektmitarbeiter
- ☐ _____

Kategorie und Art der Daten

- ☐ Dienstliche Kontaktdaten (Name, Vorname, E-Mail, Telefonnummer, Dienstanschrift)
- ☐ Private Kontaktdaten (Name, Vorname, E-Mail, Telefonnummer, Anschrift)
- ☐ Stimme als biometrisches Merkmal
- ☐ Bild als biometrisches Merkmal
- ☐ Qualifikationen (Zeugnisse, Lebenslauf, Zertifikate)
- ☐ Technische Nutzungsdaten (IP-Adresse, Betriebssystem, Browser, _____
- ☐ _____

Im Rahmen der Auftragsverarbeitung werden

☐ keine besonderen Kategorien von Daten verarbeitet.

☐ folgende besondere Kategorien von Daten im Sinne von Art. 9 DSGVO verarbeitet _____

(rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben, sexuellen Orientierung)

☐ Es erfolgt eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung gründet.

☐ Es erfolgt eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Die verarbeiteten personenbezogenen Daten haben einen

☐ normalen / ☐ hohen Schutzbedarf.

Bitte je Personenkategorie die verarbeiteten Daten benennen