Az.: B 12.23 – 0808/25/VV : 1

Vereinbarung zur Auftragsverarbeitung

- nachfolgend „Leistungsvereinbarung“ -

Zwischen der

Bundesrepublik Deutschland,

vertreten durch

die Bundeszentrale für politische Bildung, diese vertreten durch
die/den Präsidentin/Präsidenten
Bundeskanzlerplatz 2, 53113 Bonn

- nachfolgend „Verantwortlicher“ -

und

XXXXXXXXXXX

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhaltsverzeichnis

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) Diese Vereinbarung gilt vorrangig vor anderen Vereinbarungen und Abreden zwischen Auftraggeber und Auftragnehmer, es sei 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) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:
Personaldaten, wie Name, Vorname, Postanschrift; ggf. Kommunikationsdaten (E-Mails, Telefonnummern)

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist (Kategorien betroffener Personen):
in der anhängenden Leistungsbeschreibung nicht konkret, sondern allgemein beschrieben: Einzelpersonen, Schulen, Institutionen, die mit Ausgaben/Materialien der Reihe „Was geht?“ beliefert werden.

(4) Im Rahmen der Auftragsverarbeitung werden keine besonderen Kategorien von Daten verarbeitet.

(5) Die verarbeiteten personenbezogenen Daten haben einen normalen Schutzbedarf.

§ 3 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die ihnen durch datenschutzrechtliche Vorschriften (insbesondere die 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. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind im Anhang „Weisungsbefugnis“ festgelegt.

(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) 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 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 (TOM)“ wird Gegenstand dieser Vereinbarung.

(2) Ergibt eine Prüfung des Verantwortlichen einen Anpassungsbedarf der vom Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen gemäß Artikel 32 DSGVO, sind die Anpassungen vom Auftragsverarbeiter 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 (TOM)“ 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 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 DSGVO 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 dieser Vereinbarung 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 dieser Vereinbarung 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 weitere Auftragsverarbeiter (Subunternehmen) nur nach einem der nachfolgenden Verfahren einsetzen:

☒ 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.

☐ Der Auftragsverarbeiter erhält die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Subunternehmen, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Subunternehmen und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des betreffenden Subunternehmens Einwände gegen diese Änderungen erheben zu können. Der

Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann

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 bzw. seiner jeweiligen gesetzlich 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 Mitarbeiterinnen und Mitarbeiter anweisen, mit dem/der Datenschutzbeauftragten zu kooperieren, insbesondere ihre bzw. seine 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
(bitte ausfüllen)

zur Vereinbarung zur Auftragsverarbeitung vom Datum

zwischen der Bundeszentrale für politische Bildung, diese vertreten durch die/den Präsidentin/Präsidenten, Bundeskanzlerplatz 2, 53113 Bonn

und XXXXXXXXXXXXXXXXXXX

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:

- Saskia Nauck
- Sophia La Mela
- Kim Zirafi, Markus Ramscheid, Kathrin Bognár

Zum Empfang der Weisungen berechtigte Personen auf Seiten des Auftragsverarbeiters:

- Weisungsbefugter eintragen
- Stellvertreter eintragen
- Weitere Personen und Funktionen eintragen oder Zeile löschen

Vorgesehene Informationswege, wenn eine Weisung nach Meinung des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt:

☒ schriftliche und/oder

☒ 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 Bundeszentrale für politische Bildung, diese vertreten durch die/den Präsidentin/Präsidenten, Bundeskanzlerplatz 2, 53113 Bonn

und XXXXXXXXXXXX

§ 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. 32 DSGVO dienen:

Nr.	Maßnahmen	Umsetzung der Maßnahmen
1.	Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	Es werden klare Verfahrensanweisungen erstellt und veröffentlicht, wann und wie Pseudonymisierung anzuwenden ist. Dabei sind Maßnahmen vorzusehen, die sicherstellen, dass Klarnamen oder direkte Identifikatoren nach Möglichkeit durch Pseudonyme (z.B. zufällige ID oder ein Hash-Wert) ersetzt werden. Pseudonymisierten Daten werden getrennt von Zuordnungstabellen gespeichert, und nur durch befugte Dritte Personen zugänglich gemacht. Sensible Datenfelder werden durch fiktive, aber realistische Werte ersetzt und der ursprüngliche Bezug entfernt Es werden klare Richtlinien festgelegt, wer unter welchen Bedingungen Zugriff auf die Zuordnungstabelle oder die Re-Identifizierungsinstrumente erhält. Die Mitarbeiter werden durch regelmäßige Fortbildungen über den korrekten Umgang mit pseudonymisierten Daten sensibilisiert. Es ist ein sicheres und robustes Systems für die Generierung, Speicherung, Rotation und den Schutz von Verschlüsselungsschlüsseln zu implementieren. Die Schlüssel sollten separat von den verschlüsselten Daten gespeichert werden. Es sind Unternehmensrichtlinien festzulegen in dem bestimmt wird, dass alle Systeme und Daten (sofern technisch möglich) verschlüsselt sein müssen. Die Auswahl und Umsetzung dieser Maßnahmen muss sich am Stand der Technik orientieren.

Nr.	Maßnahmen	Umsetzung der Maßnahmen
2.	Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	Es sind Maßnahmen zu ergreifen, die sicherstellen, dass bei der Erfassung und Speicherung von Personaldatendaten, Adressdaten und personenbezogenen Daten - der Zugriff nur durch befugte Personen möglich ist. 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. Die Computersysteme, auf denen die Kontaktdaten erzeugt, bearbeitet und gespeichert werden, müssen angemessen vor unbefugten Zugriffen von innen und von außen geschützt sein. Es darf nur Software zum Einsatz kommen, die auf den Arbeitsrechnern oder einem lokalen Server installiert ist. Die Verwendung von mail-, internet- bzw. cloudbasierten Anwendungen ist untersagt. Es ist sicherzustellen, dass die genutzten Programme keine Dateien ins Internet übertragen und für einzelne Funktionen nicht auf Cloud-Dienste zurückgreifen.
3.	Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	Die Systeme zur Speicherung und Verarbeitung der Personaldaten, Adressdaten und personenbezogenen Daten müssen derart ausgestaltet werden, dass ein vollständiger Systemausfall soweit möglich ausgeschlossen wird. Für den Fall eines Datenverlustes muss ein Sicherungskonzept vorliegen und vollständig umgesetzt sein.
4.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	Die vereinbarten Maßnahmen werden einmal pro Vertragsjahr durch beide Parteien evaluiert. Notwendige Verbesserungen werden im beiderseitigen Einverständnis festgelegt und schriftlich festgehalten. Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können. Der Auftragnehmer muss sicherstellen, dass die bereitgestellten Personaldaten, Adressdaten und personenbezogenen Daten ausschließlich für den im Vertrag festgelegten Zweck genutzt werden.

Nr.	Maßnahmen	Umsetzung der Maßnahmen
5.	Maßnahmen zur Identifizierung und Autorisierung der Nutzer	Es ist sicherzustellen, dass Unbefugte keinen Zugang zu den Personaldaten, Adressdaten und personenbezogenen Daten erhalten und nicht auf diese zugreifen können. - Identifizierung der Nutzer durch Benutzername und Passwort - Benutzernamen werden ausschließlich verschlüsselt gespeichert - Protokollierung von Fehleingaben mit automatischer Sperre des Zugangs
6.	Maßnahmen zum Schutz der Daten während der Übermittlung	Die Daten dürfen nur über den Server übermittelt werden, der für den Austausch eingerichtet wurde. Es ist dabei sicherzustellen, dass Unbefugte keinen Zugang zu dem Server erhalten und nicht auf die Kontaktdaten zugreifen können. - Identifizierung der Nutzer durch Benutzername und Passwort - Benutzernamen werden ausschließlich verschlüsselt gespeichert - Protokollierung von Fehleingaben mit automatischer Sperre des Zugangs
7.	Maßnahmen zum Schutz der Daten während der Speicherung	Der Zugang zu den Speichersystemen muss durch technische Maßnahmen (z. B. individuelle, sichere Passwörter) auf die notwendigen Mitarbeiter beschränkt werden.
8.	Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden	Es ist sicherzustellen, dass Unbefugte keinen Zugang zu den Personaldaten, Adressdaten und personenbezogenen Daten erhalten. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Es muss sowohl eine Brand- als auch eine Einbruchmeldeanlage vorhanden sein. Es ist sicherzustellen, dass im Fall eines Brandes oder Einbruchs die Feuerwehr bzw. die Polizei zeitnah informiert wird.

Nr.	Maßnahmen	Umsetzung der Maßnahmen
9.	Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	Es ist ein Protokoll zu führen, in das alle besondere Vorkommen und Ereignisse einzutragen und der Bundeszentrale für politische Bildung mitzuteilen sind. 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.
10.	Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	Die Datenbearbeitung erfolgt ausschließlich durch Mitarbeitende, die für die Anwendung geschult sind.
11.	Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	Der Auftragnehmer befolgt Leitlinien für die Entwicklung und die Verwaltung der Software. Der Auftragnehmer verfügt über Leitlinien zum Verhalten bei Sicherheitsvorfällen und Softwarefehlern. Der Auftragnehmer führt regelmäßige Datenschutz- und Informationssicherheitsschulungen für seine Mitarbeitenden durch. Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt. Der Auftragnehmer hat einen Informationssicherheitsbeauftragten bestellt.
12.	Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	Der Auftragnehmer führt regelmäßige Datenschutz- und Informationssicherheitsschulungen durch. Fehlfunktionen werden automatisch erfasst und gemeldet.
13.	Maßnahmen zur Gewährleistung der Datenminimierung	Auf den Servern des Auftragnehmers werden die notwendigen Daten, die für die Überwachung, Replikation, Datenwiederherstellung und Abwehr von Angriffen notwendig sind gespeichert. Die hierzu gespeicherten Dateien und Backups werden nach 30 Tagen automatisch gelöscht.
14.	Maßnahmen zur Gewährleistung der Datenqualität	Es sind Maßnahmen zur Gewährleistung der Datenqualität zu ergreifen, die die Datenbereinigung, -validierung und -profilierung, die kontinuierliche Überwachung mit speziellen Tools sowie die Etablierung von Data Governance, klare Rollen, Verantwortlichkeiten und Richtlinien definieren. Darüber hinaus sind die Mitarbeiter regelmäßig zu schulen und es ist eine entsprechende Unternehmenskultur zu etablieren.

Nr.	Maßnahmen	Umsetzung der Maßnahmen
15.	Maßnahmen zur Gewährleistung einer begrenzten Speicherdauer	Systemseitige Voreinstellungen sind grundsätzlich datenschutzfreundlich („Privacy-by-default“). Die für die Abwicklung der Bestellung notwendigen Kundendaten sowie optionale Kundendaten werden bei Kündigung des Abonnements oder im Falle einer unzustellbaren Lieferung/Retoure gelöscht. Die freiwilligen Angaben zu statistischen Zwecken können darüber hinaus anonymisiert gespeichert werden.
16.	Maßnahmen zur Gewährleistung der Rechenschaftspflicht	Es ist sicherzustellen, dass auch im Fall von Urlaub, Krankheit oder anderer unerwarteter Abwesenheiten eine Ansprechperson seitens des Auftragnehmers vorhanden ist, die besondere Vorkommnisse ohne Zeitverlust der Bundeszentrale für politische Bildung mitteilt und ggf. notwendige Maßnahmen zum Schutz der Daten ergreifen kann.
17.	Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	Spätestens sechs Monate nach Beendigung des Vertragsverhältnisses mit der Bundeszentrale für politische Bildung sind die Kontaktdaten der Kundinnen und Kunden rückstandslos und nicht rekonstruierbar von allen Systemen zu löschen. Die sichere Löschung muss dokumentiert und die Dokumentation der Bundeszentrale für politische Bildung übermittelt werden. 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.

Nr.	Maßnahmen	Umsetzung der Maßnahmen
18.	Ggf. Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss	Der Auftragsverarbeiter unterstützt den Verantwortlichen aktiv, insbesondere bei: - Der Beantwortung von Anträgen betroffener Personen (z. B. Auskunft, Löschung, Datenübertragbarkeit). - Der Einhaltung der Pflichten bezüglich Meldungen von Datenschutzverletzungen an die Aufsichtsbehörden und die Betroffenen. - Datenschutz-Folgenabschätzungen und vorherigen Konsultationen mit der Aufsichtsbehörde, falls erforderlich. Spätestens sechs Monate nach Beendigung des Vertragsverhältnisses mit der Bundeszentrale für politische Bildung sind die Kontaktdaten der Kundinnen und Kunden rückstandslos und nicht rekonstruierbar von allen Systemen zu löschen. Die sichere Löschung muss dokumentiert und die Dokumentation der Bundeszentrale für politische Bildung übermittelt werden. 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.

(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) Falls vorhanden, werden folgende Nachweise 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.

(Wenn Subunternehmen vorhanden, bitte diese in die Tabelle eintragen)

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