Bundesministerium
des Innern

.

Mustervereinbarung zur

Auftragsdatenverarbeitung nach § 11 BDSG

für BMI und Geschäftsbereich

Vereinbarung zur Auftragsdatenverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [Datum]

-
- nachfolgend „Leistungsvereinbarung" -

zwischen dem

Bundesministerium des Innern (BMI)

- nachfolgend „Auftraggeber" -

und

[Vertragspartner]

- nachfolgend „Auftragnehmer" -
- beide nachfolgend gemeinsam „Vertragsparteien" -

wird die folgende Vereinbarung zur Auftragsdatenverarbeitung geschlossen:

Inhalt

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsdatenverarbeitungsverhältnis gemäß § 11 Bundesdatenschutzgesetz (BDSG) eingegangen. Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich
Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber die gemäß § 3 Abs. 7 BDSG verantwortliche Stelle ist.

§ 2 Begriffsbestimmung
Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Auftraggeber vorgegebenen Algorithmus (Auftragsdatenverarbeitung). Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

§ 3 Konkretisierung des Auftragsinhalts
(1) Der Gegenstand und die Dauer der Auftragsdatenverarbeitung (§ 11 Abs. 2 S. 2 Nr. 1 BDSG) sowie Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten (§ 11 Abs. 2 S. 2 Nr. 2 BDSG) sind in der Leistungsvereinbarung niedergelegt.

[Alternative 1 Konkretisierung der Datenarten in der Leistungsvereinbarung – *falls nicht zutreffend, bitte streichen*]
(2) Die Art der verwendeten personenbezogenen Daten ist in der Leistungsbeschreibung unter [Punkt/Ziffer/§] konkret beschrieben.
[Alternative 2 Konkretisierung der Datenarten in dieser Vereinbarung zur Auftragsdatenverarbeitung – *falls nicht zutreffend, bitte streichen*]
(2) Folgenden Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragnehmer: [Aufzählung oder Beschreibung der Datenarten oder –kategorien, z.B. Personaldaten, Kommunikationsdaten etc.].

[Alternative 1 Konkretisierung der Betroffenen in der Leistungsvereinbarung – *falls nicht zutreffend, bitte streichen*]
(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen ist in der Leistungsbeschreibung unter [Punkt/Ziffer/§] konkret beschrieben.
[Alternative 2 Konkretisierung der Betroffenen in dieser Vereinbarung zur Auftragsdatenverarbeitung – *falls nicht zutreffend, bitte streichen*]
(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst: [Aufzählung oder Beschreibung der betroffenen Personenkategorien, z.B. Beschäftigte etc.].

§ 4 Verantwortlichkeit und Weisungsbefugnis
(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (§ 3 Abs. 7 BDSG). Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen (§ 11 Abs. 2 S. 2 Nr. 4 und 10 BDSG). Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Auftraggeber danach in schriftlicher Form durch

eine einzelne Weisung geändert, ergänzt oder ersetzt werden (§ 11 Abs. 2 S. 2 Nr. 9 BDSG).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

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

(5) Der Auftraggeber führt das Verfahrensverzeichnis gem. § 4g Abs. 2 Satz 2 BDSG. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch Informationen zur Aufnahme in das Verfahrensverzeichnis zur Verfügung.

(6) Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Eine Verlagerung in einen Staat außerhalb des Hoheitsgebiets der Bundesrepublik Deutschland bedarf der vorherigen Zustimmung des Auftraggebers. Die besonderen Voraussetzungen der §§ 4b, 4c BDSG bleiben unberührt.

(7) Eine Verarbeitung von personenbezogenen Daten in Privatwohnungen der Mitarbeiter des Auftragnehmers (Telearbeitsplätze, Heimarbeitsplätze) ist nicht zulässig.

§ 5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer

(1) Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer gemäß § 11 Abs. 4 BDSG die nachfolgenden gesetzlichen Pflichten.

(2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsdatenverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

[Alternative 1 Regelung weiterer Pflichten nicht-öffentlicher Stellen / Unternehmen als Auftragnehmer – *falls nicht zutreffend, bitte streichen*]

(3) Der Auftragnehmer hat nach Maßgabe des § 4f BDSG einen Datenschutzbeauftragten zu bestellen, der seine Tätigkeit gemäß §§ 4f und 4g BDSG ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden nach § 38 BDSG oder falls eine Aufsichtsbehörde nach §§ 43, 44 BDSG bei dem Auftragnehmer ermittelt.

[Alternative 2 Regelung weiterer Pflichten öffentlicher Stellen / Behörden als Auftragnehmer, einschließlich nicht-öffentlicher Stellen, deren Anteile mehrheitlich im Besitz der öffentlichen Hand sind – *falls nicht zutreffend, bitte streichen*]

(3) Der Auftragnehmer beachtet die Durchführungsbestimmungen und die Regelungen zur Datenschutzaufsicht des jeweils einschlägigen Datenschutzgesetzes.

§ 6 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 gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG. Er ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer 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.

(3) Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

(4) Der Auftraggeber kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen (§ 11 Abs. 2 S. 2 Nr. 7 BDSG).

§ 7 Mitteilung bei Verstößen durch den Auftragnehmer

(1) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (§ 11 Abs. 2 S. 2 Nr. 8 BDSG).
(2) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 8 Löschung und Rückgabe von Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch des Auftraggebers, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis ste-

hen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten (§ 11 Abs. 2 S. 2 Nr. 10 BDSG). Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Auftraggeber auf Anforderung vorzulegen.

(3) Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 9 Subunternehmer

(1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Genehmigung des Auftraggebers vergeben werden (§ 11 Abs. 2 S. 2 Nr. 6 BDSG). Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden.

(3) Dem Auftraggeber sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

§ 10 Nebenleistungen

Die §§ 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5 BDSG).

§ 11 Datenschutzkontrolle

Der Auftragnehmer verpflichtet sich, dem/der BDS des Auftraggebers sowie dem Vertreter des BfDI zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - 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) Der Anhang „Technisch-organisatorische Maßnahmen" ist Bestandteil dieser Vereinbarung.

Datum, Ort	Datum, Ort
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
Name, Vorname, Funktion	Name, Vorname, Funktion

Bundesministerium
des Innern

Anhang „Technisch-organisatorische Maßnahmen nach § 9 BDSG

zur Vereinbarung zur Auftragsdatenverarbeitung vom [Datum] zwischen
dem Bundesministerium des Innern (BMI) und [Vertragspartner]

§ 5 der Vereinbarung zur Auftragsdatenvereinbarung verweist zur Konkretisierung der technisch-organisatorischen Datenschutzmaßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragnehmers
Der Auftragnehmer 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 personenbezogenen Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	[Ergänzen, z.B. Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte (§ 6c BDSG), Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung (§ 6b BDSG), Alarmanlage, Türsicherung]
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	[Ergänzen, z.B. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Kennwortverfahren, Automatische Sperrung, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern)]

3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	[Ergänzen, z.B. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren](Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung)
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	[Ergänzung, z.B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur]
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	[Ergänzen, z.B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Protokollauswertungssysteme]
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	[Ergänzen]Abgrenzung der Kompetenz zwischen Auftraggeber und Auftragnehmer (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragnehmers, Kontrolle der Vertragsausführung)
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	[Ergänzen, z.B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung](Beispiel: Backup-Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan)

8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	[Ergänzen, z.B. Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion / Test]

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion