

Erklärung über die Auftragsverarbeitung

1. Allgemeines

Der Auftragnehmer führt die vereinbarte Leistung gemäß der Leistungsbeschreibung vom **19.12.2025** über „**Rahmenverträge Digitale Kommunikation: Relaunch Website, Design, Hosting, Support und Weiterentwicklung - Los (bitte eintragen)**“ ausschließlich im Rahmen der getroffenen Vereinbarungen nach dem Gegenstand und der Dauer des Auftrags durch.

Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 Datenschutz-Grundverordnung (DSGVO). Diese Erklärung regelt die Rechte und Pflichten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

2. Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung ergibt sich aus der Leistungsbeschreibung. Die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in der **Anlage Teil A** zu dieser Erklärung festgelegt.

3. Verantwortlicher

Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragsverarbeiter.

4. Pflichten des Auftragsverarbeiters

Der Auftragnehmer ist Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO.

Er verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragsverarbeiter ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragsverarbeiter untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

Der Auftragsverarbeiter verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

5. Datenschutzbeauftragter

Der Auftragsverarbeiter bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragsverarbeiter trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragsverarbeiter teilt dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten auf Anforderung gesondert in Textform mit.

Die Pflicht zur Benennung eines Datenschutzbeauftragten kann entfallen, wenn der Auftragsverarbeiter nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen, und nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflicht des Auftragsverarbeiters

Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen an die Aufsichtsbehörde darf der Auftragsverarbeiter nur nach vorheriger Weisung durch den Auftraggeber durchführen.

7. Mitwirkung des Auftragsverarbeiters

Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragsverarbeiter unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12 bis 22 DSGVO.

Der Auftragsverarbeiter wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er teilt dem Auftraggeber die jeweils erforderlichen Angaben auf Anforderung in geeigneter Weise mit.

8. Kontrolle durch den Auftraggeber

Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers vor Beginn der Datenverarbeitung und sodann in regelmäßigen Abständen jederzeit im erforderlichen

Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und durch die Begehung der Räume, in denen die Arbeiten durchgeführt werden.

Der Auftragsverarbeiter ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

9. Unteraufträge

Die Beauftragung von Unterauftragnehmern durch den Auftragsverarbeiter ist nur mit vorheriger Zustimmung des Auftraggebers in Schriftform zulässig. Der Auftragsverarbeiter wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage Teil B** zu dieser Erklärung angeben.

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Unterauftragnehmern gelten.

Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt.

10. Vertraulichkeit

Der Auftragsverarbeiter ist verpflichtet, alle Informationen, die er im Zusammenhang mit der Durchführung dieses Vertrages erhält, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden.

Der Auftragsverarbeiter sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit deren Anwendung vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

11. Technisch-organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften nach einer durchgeführten Risikobeurteilung erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage Teil C** zu diesem Vertrag beigelegt.

Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht mehr genügen, benachrichtigt er den Verantwortlichen unverzüglich.

Die technischen und organisatorischen Maßnahmen beim Auftragsverarbeiter müssen im Laufe des Auftragsverhältnisses regelmäßig und anlassbezogen weiterentwickelt und angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten.

Wesentliche Änderungen sind vom Auftragsverarbeiter mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

12. Vertragsdauer

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

13. Beendigung

Nach Beendigung des Vertrages hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.

Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragsverarbeiter zu kontrollieren.

Datum, Unterschrift (Signatur oder Textform*)

Anlage

Teil A Gegenstand des Auftrags

Hier sollen beschrieben werden:

Folgende Datenarten: [Namen und Kontaktdaten, inkl. technischer Kontaktdaten wie IP-Adressen von BIBB Beschäftigten, sowie Nutzerinnen und Nutzer des BIBB-Internetangebotes.](#)

Kreis der von der Datenverarbeitung betroffenen Personen: [BIBB Beschäftigte und Nutzerinnen und Nutzer des BIBB-Internetangebotes.](#)

Teil B Unterauftragnehmer

Nennung der Unterauftragnehmer:

Name, Adresse und vorgesehene Tätigkeiten:
[vom Auftragnehmer zu erläutern](#)

Teil C Technische organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Die getroffenen Maßnahmen sind vom Auftragsverarbeiter in der Anlage oder in einem beigefügten Schreiben, das die aufgeführten Punkte berücksichtigt, möglichst konkret zu beschreiben und zu bestätigen. Die reine Angabe von Stichworten reicht nicht aus. Die genannten Fragen und Stichpunkte sind als Hinweise auf Beispiele zu verstehen. Es können auch adäquate Alternativen mit entsprechendem Sicherheitsniveau genannt werden.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Hier können Sie Angaben zu folgenden Aspekten machen:

- Wie ist der Zutritt des Gebäudes gesichert in dem die Daten verarbeitet werden?
- Gibt es einen Pförtner-Dienst?
- Gibt es eine Zutrittsregelung? Wenn ja, wie ist diese ausgestaltet?
- Gibt es eine Videoüberwachung?
- Gibt es eine Schlüsselregelung bzw. ein Zutrittskonzept? Wenn ja, wie ist diese ausgestaltet?
- Gibt es eine Alarmanlage? Was passiert im Alarmfall?
- Sonstige Maßnahmen

[vom Auftragnehmer zu erläutern](#)

1.2. Zugangskontrolle

Hier können Sie Angaben zu folgenden Aspekten machen:

- Gibt es ein Berechtigung Konzept für den Zugang System?
- Wird die Erteilung und der Entzug von Berechtigungen protokolliert? Wer hat Zugriff auf die Protokolle?
- Wie wird sichergestellt, dass nur erforderliche Berechtigungen eingeräumt werden?
- Gibt es eine Passwortrichtlinie?

- Welche Mindestpasswortlänge wird verlangt? Wird die Mindestlänge technisch erzwungen?
- Wird eine Passwortkomplexität verlangt? Wird diese technisch erzwungen?
- Wird ein Passwortwechsel erzwungen? Wenn ja, wann und wie?
- Werden externe Schnittstellen (z.B. USB) gesperrt?
- Werden mobile IT-Systeme verschlüsselt?
- Werden mobile Datenträger verschlüsselt?
- Wie werden IT-Systeme vor Viren und Schadsoftware geschützt?
- Wie werden unberechtigte Zugriffe von Dritten auf IT-Systeme erkannt und unterbunden?
- Wie wird Sorge dafür getragen, dass nur sorgfältig ausgewählte und überprüfte Dienstleister in Kontakt mit personenbezogenen Daten gelangen?
[vom Auftragnehmer zu erläutern](#)

1.3. Zugriffskontrolle

Hier können Sie Angaben zu folgenden Aspekten machen:

- Wie wird gewährleistet, dass Berechtigungen differenziert vergeben werden?
- Werden Benutzerrollen und damit einhergehende Berechtigungen regelmäßig überprüft?
- Wie wird sichergestellt, dass Rechte von Personen beim Ausscheiden aus dem Unternehmen oder beim Wechsel einer Aufgabe im Unternehmen entzogen werden?
- Haben alle Administratoren Zugriff auf alle Daten und Systeme? Oder ist die Anzahl der Administratoren auf das Notwendigste beschränkt? Wie wird dies sichergestellt?
- Werden Zugriffe auf Daten protokolliert?
- Wie wird sichergestellt, dass nicht mehr verwendete Datenträger sicher gelöscht oder vernichtet werden?
- Wie wird sichergestellt, dass Papierunterlagen mit personenbezogenen Daten sicher vernichtet werden und die Vernichtung nachgewiesen wird?
[vom Auftragnehmer zu erläutern](#)

1.4. Trennung

Hier können Sie Angaben zu folgenden Aspekten machen:

- Wie wird sichergestellt, dass Daten, die zu verschiedenen Zwecken verarbeitet werden, getrennt voneinander verarbeitet werden?
[vom Auftragnehmer zu erläutern](#)

1.5. Pseudonymisierung und Verschlüsselung

Hier können Sie Angaben zu folgenden Aspekten machen:

- Kommt eine Pseudonymisierung oder Verschlüsselung von Daten zum Einsatz? Wenn ja, beschreiben Sie dies bitte möglichst konkret.
[vom Auftragnehmer zu erläutern](#)

2. Integrität

2.1. Eingabekontrolle

Hier können Sie Angaben zu folgenden Aspekten machen:

- Wie wird gewährleistet, dass jederzeit festgestellt werden kann, wer personenbezogene Daten wie eingegeben, verändert oder gelöscht hat?
- Wie lange werden die Nachweise dieser Eingaben, Änderungen und Löschungen („Protokolle“) gespeichert?
- Gibt es Zugriffskonzepte für die Protokolldateien?
[vom Auftragnehmer zu erläutern](#)

2.2. Weitergabekontrolle

Hier können Sie Angaben zu folgenden Aspekten machen:

- Wie werden personenbezogene Daten zwischen Auftraggeber und Auftragnehmer übertragen?
- Wie wird der Schutz der Daten während des Transports gewährleistet?
- Wie wird gewährleistet, dass Daten nach der Beendigung des Auftrags sicher gelöscht werden?
- Wie wird die Löschung dokumentiert?
[\(vom Auftragnehmer zu erläutern\)](#)

3. Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit

Hier können Sie Angaben zu folgenden Aspekten machen:

- Gibt es Feuer- und Rauchmeldeanlagen? Bitte beschreiben.
- Sind Serverräume klimatisiert?
- Ist eine unterbrechungsfreie Stromversorgung (USV) im Einsatz?
- Bitte beschreiben Sie ihr Datensicherungs- und Wiederherstellungskonzept.
- Wo werden Datensicherungen aufbewahrt?
- Sind Datensicherungen verschlüsselt?
- Gibt es einen Notfallplan?
[\(vom Auftragnehmer zu erläutern\)](#)

4. Verfahren zur regelmäßigen Überprüfung der genannten Maßnahmen

Hier können Sie Angaben zu folgenden Aspekten machen:

- Hat die Unternehmensleitung Verantwortung für Datenschutz und Informationssicherheit übernommen („Leitlinie“)?
- Werden die Beschäftigten zum Datenschutz geschult? Wenn ja, wie und wie häufig?
- Werden die Beschäftigten zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet? Wie wird sichergestellt, dass alle Mitarbeiter zur Vertraulichkeit verpflichtet werden?
- Ist eine Datenschutzbeauftragte/ein Datenschutzbeauftragter benannt worden?
- Welche Maßnahmen werden zur Umsetzung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) getroffen?
- Gibt es Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten?
- Wie wird sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden?
- Gibt es ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO?
- Welche Maßnahmen sind ansonsten getroffen worden, um die Umsetzung der Vorgaben der DSGVO im Unternehmen zu gewährleisten?
- Ist ein Datenschutzmanagementsystem (DSMS) implementiert worden?
[\(vom Auftragnehmer zu erläutern\)](#)

Datum, Unterschrift (Signatur oder Textform*)

*) lesbare Erklärung in der das Unternehmen oder die handelnde Person genannt wird