**ARBEITSMATERIAL**

**2/7 VORLAGE Auftragsverarbeitungsvertrag**

aus: Datenbank und Datenschutz gehören zusammen

Die Themenreihe „**Datenbank und Datenschutz gehören zusammen**“

ist eine Kooperation mit Dirk Wolf,

dem Datenschutzbeauftragten des Deutschen Fundraising-Verbandes (DFRV).

Sie erreichen Dirk Wolf

für Rückfragen und Buchung

unter: wolf@skriptura.de

DATENWELTEN bietet Ihnen als kostenfreie Basics:

1. MUSTER Verzeichnis von Verarbeitungstätigkeiten (VVT)
2. VORLAGE Auftragsverarbeitungsvertrag (AVV)
3. MUSTER Liste der Technische und organisatorische Maßnahmen (TOM)
4. MUSTER-Datenschutzrichtlinie
5. PODCAST (ab März 2023): Die gängigsten Datenschutz-Pannen bei der Nutzung einer Fundraising-Datenbank
6. Zum Nachschlagen „Aufbewahrungsfristen“

Des Weiteren finden Sie im Shop:

1. VIDEO (ab März 2023)

****Die zehn wichtigsten ToDos für eine DSGVO-konforme Datenbank-Nutzung

**Vereinbarung gemäß Artikel 28 Abs. 3
Europäische Datenschutz-Grundverordnung
(im Folgenden DSGVO)**

zwischen dem/der

Auftraggeber GmbH
Straße HsNr
PLZ Ort

vertreten durch …

nachstehend Auftraggeber genannt - und dem/der

Auftragnehmer oHG
Straße HsNr
PLZ Ort

vertreten durch …

nachstehend Auftragnehmer genannt

**1. Gegenstand und Dauer des Auftrags**

**(1) Gegenstand**

Gegenstand des Auftrags zum Datenumgang ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag und nach Weisung des Auftraggebers.

**(2) Dauer**

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien jederzeit mit einer Frist von vier Wochen gekündigt werden. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt hiervon unberührt.

**2. Konkretisierung des Auftragsinhalts:**

**(1) Art und Zweck der vorgesehenen Verarbeitung von Daten**

Beispiel: Personalisierung und Versand von Spendenaufrufen im Auftrag des Auftraggebers: Erstellen von Anweisungen für die Mailingaufbereitung, den Laserprint und Postversand, Kontrolle von personalisierten Laserandrucken, Weitergabe der personalisierten Laserandrucke an den Auftraggeber zur Freigabe, Freigabe der Laserandrucke an den Lettershop, Prüfung und Freigabe von personalisierten Kuvertiermustern.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

**(2) Art der Daten**

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

Beispiel:

Adressdaten

Kommunikationsdaten (z.B. Telefon, E-Mail)

Vertragsabrechnungs- und Zahlungsdaten

**(3) Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Beispiel:

Kunden/Spender

Interessenten

Inaktive Kunden/Spender

**3. Technisch-organisatorische Maßnahmen**

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artikel 28 Abs. 3 Buchstabe c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

**4. Berichtigung, Einschränkung und Löschung von Daten**

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

**5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer werden … benannt.

Alternativ: Als Datenschutzbeauftragte wurde benannt:

Frau DSB

Straße HsNr
PLZ Ort

Tel.:

E-Mail:

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artikel 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Artikel 28 Abs. 3 S. 2 Buchstabe b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Abs. 3 S. 2 Buchstabe c, 32 DSGVO [Einzelheiten in Anlage 1].

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

**6. Unterauftragsverhältnisse**

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nach eigenem Ermessen beauftragen.

Alternative 1: (2) Der Aufragnehmer darf Unterauftragnehmer nicht in Anspruch nehmen.

Alternativ: (2) Der Aufragnehmer darf Unterauftragnehmer nach vorheriger Absprache 2 und Genehmigung durch den Auftraggeber in Anspruch nehmen. Derzeit sind folgende Unterauftragnehmer genehmigt:

 Unternehmen A

 Unternehmen B

 …

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Wenn Alternative 2 nicht in Anspruch genommen wird: (5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

**7. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

**8. Mitteilung bei Verstößen des Auftragnehmers**

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

**9. Weisungsbefugnis des Auftraggebers**

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

**10. Löschung und Rückgabe von personenbezogenen Daten**

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Ort/Datum Ort/Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
- Auftraggeber - - Auftragnehmer -

**Anlage Technische und organisatorische Maßnahmen**

1. Vertraulichkeit (Art. 32 Abs. 1 Buchstabe b DSGVO)

* Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

* Manuelles Schließsystem
* Protokollierung des Zutritts zum Serverraum
* Zugangskontrolle
* Dedizierte Benutzerprofile pro PC
* Authentifizierung durch Benutzername und Passwort
* Einsatz von Antiviren-Software
* Einsatz einer Hardware-Firewall
* Zugriffskontrolle

Maßnahmen, die 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.

* + Berechtigungskonzept vorhanden
	+ Rechteverwaltung durch Systemadministrator
	+ Nur ein Administrator-Account vorhanden
	+ Sichere Löschung von Daten auf Festplatten und SSDs mit Software nach Standards US Army AR380-19, DoD 5220.22-M ECE, DoD 5220.22-M E, US Air Force System Security 5020, NATO Standard, US Navy NAVSO P-5239-26 und CSEC ITSG-06, auf Wunsch mit Löschprotokoll

2. Integrität (Art. 32 Abs. 1 Buchstabe b DSGVO)

* Weitergabekontrolle

Maßnahmen, die 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.

* + Verschlüsselung von eMail-Anhängen
	+ Protokollierung von Abruf- und Übermittlungsvorgängen per FTP
* Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

* Berechtigungskonzept zur Eingabe, Änderung und Löschung von Daten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchstabe b DSGVO)

* Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

* USV in Serverräumen
* Klimaanlage im Serverraum
* Temperaturüberwachung im Serverraum
* Schutzsteckdosenleisten im Serverraum
* Feuer- und Rauchmeldeanlagen
* Feuerlöschgeräte im Serverraum
* Datenwiederherstellung wird stichprobenartig getestet
* Notfallplan vorhanden
* Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
* 24h-Überwachung von Servern