**ARBEITSMATERIAL**

**4/7 MUSTER Datenschutzrichtlinie**

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

*Diese Vorlage einer Datenschutzrichtlinie dient lediglich als „Gerüst“. Sie muss Satz für Satz bearbeitet und auf die Verhältnisse in Ihrer Organisation angepasst werden.*

**Datenschutzrichtlinie**

**Organisation**

# Vorwort

*Einige Worte zu Ihrer Organisation und der grundlegenden Einstellung zum Datenschutz, der in Ihrer Organisation vorherrscht.*

In unserer Datenschutzrichtlinie haben wir strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von **Subjekten des Datenschutzes**, Geschäftspartnern und Mitarbeiter\*innen geregelt. Diese entspricht den Anforderungen der Europäischen Datenschutz-Grundverordnung, stellt die Einhaltung der Prinzipien der Datenschutzgesetze sicher und regelt den Datenaustausch mit Partnern, die uns Ihre Daten anvertrauen. Als Maßstab haben wir in Übereinstimmung mit der Europäischen Datenschutz-Grundverordnung sieben Datenschutzgrundsätze festgelegt:

1. Rechtmäßigkeit, Treu und Glauben, Transparenz
2. Zweckbindung
3. Datenminimierung- und Sparsamkeit
4. Richtigkeit
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit
7. Rechenschaftspflicht

Unsere Mitarbeiter\*innen sind verpflichtet, diese Datenschutzrichtlinie einzuhalten und die jeweiligen europäischen und deutschen Datenschutzgesetze zu wahren. Als **Geschäftsführer/in** **/ Vorstand** trage ich dafür Sorge, dass diese Bestimmungen zum Datenschutz **in Organisation** geachtet werden.

Meine Mitarbeiter\*innen und ich stehen Ihnen als Ansprechpartner bei Fragen zum Datenschutz und zur Datensicherheit gerne zur Verfügung.

**Name**

**Geschäftsführer/in Vorstand**

Inhalt

[Vorwort 2](#_Toc33347099)

[I. Ziele der Datenschutzrichtlinie 5](#_Toc33347100)

[II. Geltungsbereich der Datenschutzrichtlinie 5](#_Toc33347101)

[III. Geltung europäischen und staatlichen deutschen Rechts 5](#_Toc33347102)

[IV. Prinzipien für die Verarbeitung personenbezogener Daten 5](#_Toc33347103)

[1. Rechtmäßigkeit, Treu und Glauben, Transparenz 5](#_Toc33347104)

[2. Zweckbindung 5](#_Toc33347105)

[3. Datenminimierung und Speicherbegrenzung 5](#_Toc33347106)

[4. Richtigkeit 5](#_Toc33347107)

[5. Integrität und Vertraulichkeit 5](#_Toc33347108)

[V. Informationspflichten bei der Erhebung personenbezogener Daten 6](#_Toc33347109)

[1. Erhebung personenbezogener Daten bei der betroffenen Person 6](#_Toc33347110)

[1.1. Erhebung personenbezogener Daten 6](#_Toc33347111)

[1.2 Faire und transparente Verarbeitung 6](#_Toc33347112)

[2. Erhebung personenbezogener Daten nicht bei der betroffenen Person 6](#_Toc33347113)

[VI. Zulässigkeit der Datenverarbeitung 6](#_Toc33347114)

[1. Kunden­ und Partnerdaten 6](#_Toc33347115)

[1.1 Datenverarbeitung für eine vertragliche Beziehung 6](#_Toc33347116)

[1.2 Datenverarbeitung zu Werbezwecken 6](#_Toc33347117)

[1.3 Einwilligung in die Datenverarbeitung 7](#_Toc33347118)

[1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis 7](#_Toc33347119)

[1.5 Datenverarbeitung aufgrund berechtigten Interesses 7](#_Toc33347120)

[1.6 Verarbeitung besonderer Kategorien personenbezogener Daten 7](#_Toc33347121)

[1.7 Nutzerdaten und Internet 7](#_Toc33347122)

[2. Mitarbeiterdaten 8](#_Toc33347123)

[2.1 Datenverarbeitung für das Arbeitsverhältnis 8](#_Toc33347124)

[2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis 8](#_Toc33347125)

[2.3 Einwilligung in die Datenverarbeitung 8](#_Toc33347126)

[2.4 Datenverarbeitung aufgrund berechtigten Interesses 8](#_Toc33347127)

[2.5 Verarbeitung besonderer Kategorien personenbezogener Daten 9](#_Toc33347128)

[2.6 Telekommunikation und Internet 9](#_Toc33347129)

[VII. Übermittlung personenbezogener Daten 9](#_Toc33347130)

[VIII. Auftragsdatenverarbeitung 10](#_Toc33347131)

[IX. Rechte des Betroffenen 10](#_Toc33347132)

[X. Vertraulichkeit der Verarbeitung 11](#_Toc33347133)

[XI. Sicherheit der Verarbeitung 11](#_Toc33347134)

[XII. Datenschutzkontrolle 11](#_Toc33347135)

[XIII. Datenschutzvorfälle 12](#_Toc33347136)

[XIV. Verantwortlichkeiten und Sanktionen 12](#_Toc33347137)

[XV. Der Datenschutzbeauftragte 12](#_Toc33347138)

[Anlage Technische und organisatorische Maßnahmen \* 14](#_Toc33347139)

[1. Vertraulichkeit (Art. 32 Abs. 1 Buchstabe b DSGVO) 14](#_Toc33347140)

[o Zutrittskontrolle 14](#_Toc33347141)

[o Zugangskontrolle 14](#_Toc33347142)

[o Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. 14](#_Toc33347143)

[o Zugriffskontrolle 14](#_Toc33347144)

[o Trennungskontrolle 14](#_Toc33347145)

[o Pseudonymisierung (Art. 32 Abs. 1 Buchstabe a DSGVO; Art. 25 Abs. 1 15](#_Toc33347146)

[2. Integrität (Art. 32 Abs. 1 Buchstabe b DSGVO) 15](#_Toc33347147)

[o Weitergabekontrolle 15](#_Toc33347148)

[o Eingabekontrolle 15](#_Toc33347149)

[3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchstabe b DSGVO) 15](#_Toc33347150)

[o Verfügbarkeitskontrolle 15](#_Toc33347151)

[o Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchstabe d DSGVO; Art. 25 Abs. 1 DSGVO) 16](#_Toc33347152)

# I. Ziele der Datenschutzrichtlinie

***Organisation*** verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutzrichtlinie beruht auf den akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation des Organisation s als anerkannte Stiftung.

Die Datenschutzrichtlinie schafft eine der notwendigen Rahmenbedingungen für Datenübermittlungen. Sie gewährleistet das von der Europäischen Datenschutz-Grundverordnung und den nationalen Gesetzen verlangte angemessene Datenschutzniveau.

# II. Geltungsbereich der Datenschutzrichtlinie

Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten.

Die jeweils aktuelle Version der Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf der Internetseite ***Organisation****,* ***www.organisation.de/datenschutz***, abgerufen werden.

# III. Geltung europäischen und staatlichen deutschen Rechts

Diese Datenschutzrichtlinie gründet auf der Europäischen Datenschutz-Grundverordnung, dem deutschen Bundesdatenschutzgesetz und weiteren Gesetzen und Verordnungen. Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen werden beachtet.

# IV. Prinzipien für die Verarbeitung personenbezogener Daten

## 1. Rechtmäßigkeit, Treu und Glauben, Transparenz

Jegliche Verarbeitung personenbezogener Daten bedarf einer dokumentierten Rechtsgrundlage. Wir verarbeiten personenbezogene Daten ausschließlich nach Treu und Glauben, das heißt in einer fairen Art und Weise, was transparentes Handeln voraussetzt.

## 2. Zweckbindung

Die Erhebung und Verarbeitung personenbezogener Daten erfolgt ausschließlich für vorher festgelegte, eindeutige und legitime Zwecke. Eine Weiterverarbeitung für andere Zwecke ist ausschließlich im Rahmen von Art. 6 Abs. 4 DS-GVO gestattet.

## 3. Datenminimierung und Speicherbegrenzung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Daten, die nicht benötigt werden, werden nicht erhoben oder, wenn sie nicht mehr benötigt werden, gelöscht.

## 4. Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein, sind sie im Hinblick auf die Zwecke der Verarbeitung unrichtig, müssen sie unverzüglich berichtigt oder gelöscht werden.

## 5. Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung. Dies wird gewährleistet durch geeignete technische und organisatorische Maßnahmen (siehe Anlage 1).

# V. Informationspflichten bei der Erhebung personenbezogener Daten

## 1. Erhebung personenbezogener Daten bei der betroffenen Person

### 1.1. Erhebung personenbezogener Daten

Werden durch ***Organisation*** personenbezogene Daten bei der betroffenen Person erhoben, ist dieser mitzuteilen, dass ***Organisation*** für die rechtmäßige Verarbeitung dieser Daten verantwortlich ist. Die Kontaktdaten des Datenschutzbeauftragten (siehe XV. dieser Datenschutzrichtlinie) sind der betroffenen Person mitzuteilen. Die Zwecke, für die ***Organisation*** die Daten erhebt sowie die Rechtsgrundlage für die Verarbeitung sind zu nennen, ebenso wie eventuelle Empfänger der Daten und, falls das beabsichtigt ist, dass die Daten in ein Land übermittelt werden sollen, das nicht der Europäischen Union angehört (Drittland). Geplante Übermittlungen in ein Drittland sind ohne eine Genehmigung der Geschäftsführung nicht gestattet. Die Geschäftsführung wird sich mit dem Datenschutzbeauftragten dazu besprechen.

### 1.2 Faire und transparente Verarbeitung

Um eine faire und transparente Verarbeitung personenbezogener Daten zu gewährleisten, ist der betroffenen Person mitzuteilen, wie lange die Daten gespeichert werden sollen. Es ist darauf hinzuweisen, dass die betroffene Person ein Recht hat, Auskunft zu erlangen über die von ihr gespeicherten Daten. Es ist auch darauf hinzuweisen, dass sie ein Recht hat ihre Daten berichtigen zu lassen, sie löschen zu lassen oder ihrer Nutzung zu Werbezwecken zu widersprechen. Wenn die betroffene Person in die Verarbeitung ihrer Daten eigewilligt hat, hat sie das Recht, diese Einwilligung zu widerrufen. Außerdem ist ihr mitzuteilen, dass sie das Recht hat, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung ihrer personenbezogenen Daten durch die Stiftung zu beschweren.

## 2. Erhebung personenbezogener Daten nicht bei der betroffenen Person

Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, ist dieser spätestens innerhalb eines Monats zusätzlich zu den in V.1. genannten Punkten mitzuteilen, welche Kategorien von Daten verarbeitet werden sollen.

# VI. Zulässigkeit der Datenverarbeitung

## 1. Kunden­ und Partnerdaten

### 1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten der Betroffenen *(****Subjekte des Datenschutzes****)* dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden (Art. 6 Abs. 1 (b) DS-DS-GVO). Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche erlaubt. Betroffene dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Betroffenen geäußerte Einschränkungen sind zu beachten. Für darüberhinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter V.1.2 beachtet werden.

### 1.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an ***Organisation*** (z.B. Wunsch nach Zusendung von Informationsmaterial), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig (Art. 6 Abs. 1 (b) DS-GVO).

Darüberhinausgehende Kundenbindungs­ oder Spendenmaßnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken des Fundraisings oder der Markt­ und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Spendenwerbung zu informieren. Sofern Daten ausschließlich für Spendenwerbung erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene ist über die Freiwilligkeit der Angabe von Daten für diese Zwecke zu informieren. Im Rahmen der Interessensabwägung (Art. 6 Abs. 1 (f) DS-GVO) ist keine ausdrückliche Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Spendenwerbezwecken einzuholen. Der Betroffene kann im Rahmen einer Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen (Einwilligung s. V.1.3).

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Spendenwerbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden.

### 1.3 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden (Art. 6 Abs. 1 (a) DS-GVO). Vor der Einwilligung muss der Betroffene gemäß IV.2. dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

### 1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

### 1.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses von ***Organisation*** erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Einwerbung von Spenden). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für die Verarbeitung zu prüfen.

### 1.6 Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonderer Kategorien personenbezogener Daten geplant, ist der Datenschutzbeauftragte im Vorfeld einzubeziehen.

### 1.7 Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten verarbeitet werden, ist von den Betroffenen vor der Verarbeitung eine Einwilligung einzuholen. Die Einwilligungen sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig anzupassen sind.

Sollen zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking) werden, so müssen die Betroffenen dazu vor der Erstellung ihre Einwilligung erteilen.

Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

## 2. Mitarbeiterdaten

### 2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des/der Bewerbers/in unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der/die Bewerber/in hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt.
Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder Weitergabe in weitere Abteilungen erforderlich. Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift. Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den/die Bewerber/in bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des/der Betroffenen einzuholen. Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen der Stiftung sein.

### 2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten von Mitarbeiter\*innen ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des/der Mitarbeiters in berücksichtigt werden.

### 2.3 Einwilligung in die Datenverarbeitung

Eine Verarbeitung personenbezogener Daten von Mitarbeiter\*innen kann aufgrund einer Einwilligung des/der Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutzrichtlinie informiert werden.

### 2.4 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten von Mitarbeiter\*innen kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der ***Organisation*** erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich begründet. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des/der Mitarbeiters in das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen. Kontrollmaßnahmen, die eine Verarbeitung personenbezogener Daten von Mitarbeiter\*innen erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen der ***Organisation*** an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und interner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des/der von der Maßnahme betroffenen Mitarbeiters/in am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse der ***Organisation*** und die möglichen schutzwürdigen Interessen des/der Mitarbeiter/in müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

### 2.5 Verarbeitung besonderer Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besondere Kategorien personenbezogener Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder weltanschauliche Überzeugungen, über Gewerkschaftszugehörigkeiten, über die Gesundheit, das Sexualleben oder die sexuelle Orientierung des Betroffenen sowie dessen genetische Daten und biometrische Daten zur eindeutigen Identifizierung natürlicher Personen. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der/die Mitarbeiter/in kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Die Einwilligung muss sich auf die Verarbeitung besonderer Kategorien personenbezogener Daten beziehen.

### 2.6 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und ***Organisationsressource***. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der ***Organisation*** internen Richtlinien genutzt werden. Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. Internet-Nutzung findet statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer sind Schutzmaßnahmen an den Übergängen in das ***Organisation***-Netzwerk implementiert worden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit und Nachvollziehbarkeit wird die Nutzung der Telefonanlagen, der E-Mail-Adressen und des Internets sowie der internen sozialen Netzwerke protokolliert. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der ***Organisation*** erfolgen. Diese Kontrollen dürfen nur unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden internen Regelungen. Die Auswertungen dienen nicht der Leistungserfassung.

# VII. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb oder innerhalb der ***Organisation*** unterliegen den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt V. Etwaige Empfänger der personenbezogenen Daten müssen darauf verpflichtet werden, diese nur zu den festgelegten Zwecken rechtmäßig zu verwenden.

Im Falle einer Datenübermittlung an einen Empfänger außerhalb der ***Organisation*** muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt.

Im Falle einer Datenübermittlung von Dritten an die Stiftung muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

Im Fall eines von einem Betroffenen behaupteten Verstoßes gegen diese Datenschutzrichtlinie verpflichtet sich die ***Organisation***, den Betroffenen sowohl bei der Sachverhaltsaufklärung zu unterstützen als auch die Durchsetzung seiner Rechte gemäß dieser Datenschutzrichtlinie sicherzustellen. Bei einem behaupteten Verstoß muss die ***Organisation*** gegenüber dem Betroffenen den Nachweis erbringen, dass ihr bei einer Weiterverarbeitung der erhaltenen Daten ein Verstoß gegen diese Datenschutzrichtlinie nicht zuzurechnen ist.

# VIII. Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsverarbeitung abzuschließen. Dabei behält die Stiftung die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

2. Der Auftrag ist in Textform zu erteilen, auch elektronisch. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.

3. Die von der Stiftung für den Datenschutz bereitgestellten Vertragsstandards müssen beachtet werden.

4. Bei einer Auftragsverarbeitung in einem Drittstaat sind die Anforderungen für eine Weitergabe personenbezogener Daten in Drittländer zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:

a. Vereinbarung der EU­Standardvertragsklauseln zur Auftragsverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.

b. Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus.

c. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die EU-Kommission.

# IX. Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Spendenwerbung oder der Markt­ und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

5. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

# X. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Verarbeitung ist den Mitarbeitern und den Mitarbeiterinnen untersagt. Unbefugt ist jede Verarbeitung, die vorgenommen wird, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Mitarbeiter\*innen dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter\*innen dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetzte müssen ihre Mitarbeiter\*innen bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

# XI. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT­Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Der Datenschutzbeauftragte ist einzubeziehen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen anzupassen

# XII. Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt der Geschäftsführung. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

# XIII. Datenschutzvorfälle

Jede Mitarbeiterin / jeder Mitarbeiter soll ihrem / seinem jeweiligen Vorgesetzten unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden. Diese/r ist verpflichtet, die Geschäftsführung umgehend über Datenschutzvorfälle zu unterrichten.

Wird der Schutz personenbezogener Daten verletzt, ist der Datenschutzbeauftragte unverzüglich zu informieren. Die Geschäftsführung erfüllt in diesem Fall ihre Meldepflichten von Datenschutzvorfällen gemäß der DS-GVO.

# XIV. Verantwortlichkeiten und Sanktionen

Die Geschäftsführung ist für die Datenverarbeitung verantwortlich. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in dieser Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. Meldepflichten). Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter\*innen. Bei Datenschutzkontrollen durch Behörden sind die Geschäftsführung und der Datenschutzbeauftrage umgehend zu informieren.

Die Geschäftsführung benennen dem Datenschutzbeauftragten eine Datenschutzkoordinatorin. Die Datenschutzkoordinatorin ist Ansprechpartnerin für den Datenschutz. Sie kann Kontrollen durchführen und Mitarbeiter\*innen mit den Inhalten der Datenschutzrichtlinien vertraut machen. Die Geschäftsführung ist verpflichtet, den Datenschutzbeauftragten und die Datenschutzkoordinatorin in ihrer Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen die Datenschutzkoordinatorin und den Datenschutzbeauftragten vor Beginn der Verarbeitung über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Mitarbeiter\*innen müssen im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht können strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter\*innen verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

# XV. Der Datenschutzbeauftragte

Der Datenschutzbeauftragte als externes, fachlich weisungsunabhängiges Organ unterrichtet und berät die Geschäftsführung hinsichtlich ihrer Pflichten nach der DS-GVO, dem BDSG und weiteren relevanten Vorschriften. Er überwacht deren Einhaltung. Er ist tätig als Anlaufstelle für die Aufsichtsbehörden und arbeitet mit diesen zusammen. Der Datenschutzbeauftragte wird von der Geschäftsführung benannt.

Die Datenschutzkoordinatorin unterrichtet den Datenschutzbeauftragten zeitnah über Datenschutzrisiken.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten oder an die Datenschutzkoordinatorin wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Kann die Datenschutzkoordinatorin einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzrichtlinien nicht abstellen, muss sie den Datenschutzbeauftragten einschalten. Die Ratschläge des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung sind durch die Geschäftsführung zu berücksichtigen. Anfragen von Aufsichtsbehörden sind immer auch dem Datenschutzbeauftragten zur Kenntnis zu bringen.

Der Datenschutzbeauftragte kann wie folgt erreicht werden:

skriptura dialog systeme GmbH

Dirk Wolf

Wohlenbergstraße 6

30179 Hannover

Tal.: 0511/54294-44

Mobil: 0171/3831577

E-Mail: dirk.wolf@skriptura.de