

HINWEISE ZUM AUSFÜLLEN DER VEREINBARUNG

Für den Auftragnehmer:

1. Firmendaten eintragen:

- Tragen Sie Ihre Firmendaten im Vertragskopf unter „Auftragsverarbeiter“ ein. Dies umfasst den Namen Ihrer Firma, die Rechtsform, die Anschrift und den Vertreter.

2. Angaben in den Vertragsziffern:

- Ergänzen Sie die folgenden Ziffern im Vertrag:
 - **1.1:** Geben Sie den Gegenstand des Auftrags an, d.h., was genau Sie für den Auftraggeber verarbeiten werden.
 - **2.1:** Beschreiben Sie die Art und den Zweck der Datenverarbeitung.
 - **2.2:** Geben Sie an, welche Art von personenbezogenen Daten verarbeitet wird (z.B. Namen, Adressen, E-Mail-Adressen).
 - **2.3:** Listen Sie die Kategorien betroffener Personen auf (z.B. Kunden, Mitarbeiter).
 - **5a):** Benennen Sie Ihren Datenschutzbeauftragten oder geben Sie an, wenn keiner erforderlich ist.

3. Technische und organisatorische Maßnahmen (TOM):

- Nutzen Sie die in **Anlage 1** vorgeschlagenen TOM als Vorlage. Sie können auch Ihre eigenen Maßnahmen zur Verfügung stellen, sofern sie den Anforderungen entsprechen.

4. Liste der Unterauftragnehmer:

- Geben Sie in **Anlage 2** alle Unterauftragnehmer an, die Sie zur Erfüllung dieses Auftrags einsetzen werden. Dies beinhaltet den Namen der Firma, die Rechtsform, Kontaktdaten, die Anschrift und eine kurze Beschreibung der jeweiligen Leistungen.

5. Kontaktdaten für Rückfragen:

- Tragen Sie auf der letzten Seite Ihre Kontaktdaten ein, damit bei Rückfragen schnell Kontakt zu Ihnen aufgenommen werden kann.

6. Übermittlung des ausgefüllten Vertrags:

- Senden Sie den ausgefüllten Vertrag an Ihren Ansprechpartner beim DRK e.V., von dem Sie diesen Vertrag erhalten haben und zusätzlich an die E-Mail-Adresse datenschutz-gs@drk.de.

7. Rückmeldung:

- Nach Prüfung durch das DRK e.V. erhalten Sie eine Rückmeldung.

Für den Auftraggeber (Deutsches Rotes Kreuz e.V.):

1. Verantwortung für den Vertragsabschluss:

- Stellen Sie sicher, dass für jede Auftragsverarbeitung ein Auftragsverarbeitungsvertrag (AVV) abgeschlossen wird. Lassen Sie vom Datenschutzbeauftragten überprüfen, ob ein Vertrag erforderlich ist.

2. Überprüfung der Angaben des Auftragnehmers:

- Prüfen Sie die Angaben des Auftragnehmers zu den Ziffern 1, 2 und 5 auf inhaltliche Richtigkeit und Vollständigkeit.

3. Finale Prüfung durch den Datenschutzbeauftragten:

- Übermitteln Sie die vollständige Vereinbarung samt Anlagen zur finalen Prüfung an den Datenschutzbeauftragten über die E-Mail-Adresse datenschutz-gs@drk.de.

4. Rückfragen:

- Bei Rückfragen steht Ihnen der Datenschutzbeauftragte des DRK e.V. unter der E-Mail-Adresse datenschutz-gs@drk.de zur Verfügung.

Vielen Dank für Ihre Kooperation!

Vereinbarung zur Auftragsverarbeitung

zwischen

Deutsches Rotes Kreuz e.V.

Carstennstraße 58, 12205 Berlin,

vertreten durch den Vorstand,

dieser vertreten d.d. Vorsitzenden (Generalsekretär) Christian Reuter

- **Verantwortlicher** -

- nachstehend auch „**Auftraggeber**“ genannt -

und

[Firma Rechtsform

Anschrift

vertreten durch]

- **Auftragsverarbeiter** -

- nachstehend auch „**Auftragnehmer**“ genannt -

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Vereinbarung [Bezeichnung der Vereinbarung, z.B. „Leistungsvereinbarung“] vom TT.MM.JJJJ., auf die hier verwiesen wird (im Folgenden: Leistungsvereinbarung);

oder

☐ Auf Grundlage dieses Vertrags erfolgt eine Verarbeitung der vom Verantwortlichen überlassenen Datensätze aus folgendem Anlass: [Beschreibung des Verarbeitungsanlasses, z.B. „zur Durchführung von Marketingkampagnen“].

1.2. Dauer

Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages. Der Auftraggeber kann diese Vereinbarung sowie den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragsverarbeiter:

- die Daten des Verantwortlichen für andere als die nach dieser Vereinbarung bestimmten Zwecke verwendet;
- gegen eine wesentliche Pflicht aus dieser Vereinbarung verstößt (z.B. bei einem Datenverlust oder bei einer verschuldeten Möglichkeit der unberechtigten Kenntnisnahme durch Dritte).

Weiter ist der Verantwortliche auch bei Nichtvorliegen der Voraussetzungen gem. Satz 2 und 3 berechtigt, diese Vereinbarung und den Hauptvertrag fristlos zu kündigen, wenn der Auftragsverarbeiter wiederholt gegen diese Vereinbarung verstößt. Ein wiederholter Verstoß liegt vor, wenn der Auftraggeber den Auftragsverarbeiter mindestens zweimal schriftlich oder in Textform auf einen Verstoß hingewiesen hat und der Auftragsverarbeiter innerhalb einer angemessenen Frist keine Abhilfe geschaffen hat.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom TT.MM.JJJJ .

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: [detaillierte Beschreibung einfügen].

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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Textform und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO);

☐ wird hergestellt durch sonstige Maßnahmen [Beschreibung der Maßnahmen]: (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO).

2.2. Art der Daten

- ☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: [Beschreibung]

oder

- ☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunftsteilen)
- ☐ [Sonstige Ergänzungen]

2.3. Kategorien betroffener Personen

- ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

oder

- ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ [Sonstige Ergänzungen]

3. Technisch-organisatorische Maßnahmen

3.1. Dokumentation und Prüfung

Der Auftragnehmer dokumentiert die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung und übergibt diese dem Auftraggeber zur Prüfung (Anlage 1). Nach Akzeptanz durch den Auftraggeber werden die Maßnahmen Grundlage des Auftrags. Anpassungsbedarf wird einvernehmlich umgesetzt und dokumentiert.

3.2. Regelmäßiger Nachweis der Maßnahmen

Der Auftragnehmer weist mindestens alle zwei Jahre sowie jederzeit auf Anforderung des Auftraggebers schriftlich nach, dass er die technischen und organisatorischen Sicherheitsmaßnahmen einhält. Der Nachweis umfasst detaillierte Beschreibungen der Maßnahmen, Auditprotokolle oder Zertifikate.

3.3. Sicherheitsanforderungen gemäß DS-GVO

Der Auftragnehmer gewährleistet die Sicherheit gemäß Art. 28 Abs. 3 lit. c und Art. 32 DS-GVO, insbesondere hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, unter Berücksichtigung des Stands der Technik, Implementierungskosten, Art, Umfang und Zweck der Verarbeitung sowie der Risikoeinschätzung gemäß Art. 32 Abs. 1 DS-GVO.

3.4. Anpassungen aufgrund technischer Fortschritte

Aufgrund des technischen Fortschritts sowie der zu erwartenden Entwicklungen in der Gesetzgebung kann sich eine Notwendigkeit der Anpassung der getroffenen technischen und organisatorischen Maßnahmen ergeben. Der Auftragnehmer ist berechtigt, alternative adäquate Maßnahmen umzusetzen, vorausgesetzt, dass das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer verpflichtet sich, erforderliche Anpassungen der technischen und organisatorischen Maßnahmen an geänderte gesetzliche Vorgaben unverzüglich umzusetzen.

4. Berichtigung, Einschränkung und Löschung von Daten

- 4.1. Der Auftragnehmer darf die im Auftrag verarbeiteten Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter.
- 4.2. Der Auftragnehmer stellt die Betroffenenrechte, insbesondere ein Löschkonzept, das Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers sicher, soweit technisch möglich und rechtlich notwendig.

5. Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insbesondere gewährleistet er die Einhaltung folgender Vorgaben:

a) Datenschutzbeauftragter

Der Auftragnehmer bestellt einen Datenschutzbeauftragten gemäß Art. 38 und 39 DS-GVO. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☐ Datenschutzbeauftragte(r) [Name, Organisationseinheit, Telefon, E-Mail]:

☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.
Ansprechpartner: [Name, Organisationseinheit, Telefon, E-Mail]

☐ Der Auftragnehmer mit Sitz außerhalb der Union benennt folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO: [Name, Organisationseinheit, Telefon, E-Mail]

b) Wahrung der Vertraulichkeit

Der Auftragnehmer setzt nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet sind und zuvor mit den relevanten Datenschutzbestimmungen vertraut gemacht wurden. Personenbezogene Daten werden nur gemäß der Weisung des Auftraggebers verarbeitet.

c) **Zusammenarbeit mit der Aufsichtsbehörde**

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

d) **Information über Kontrollhandlungen**

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer Behörde, soweit sie sich auf diesen Auftrag beziehen.

e) **Unterstützung des Auftraggebers**

Der Auftragnehmer unterstützt den Auftraggeber nach besten Kräften bei Kontrollen durch die Aufsichtsbehörde, Ordnungswidrigkeits- oder Strafverfahren, Haftungsansprüchen von betroffenen Personen oder anderen Ansprüchen im Zusammenhang mit der Auftragsverarbeitung.

f) **Unterstützung bei Pflichten gemäß Art. 32 bis 36 DS-GVO**

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Pflichten aus Art. 32 bis 36 DS-GVO.

6. Unterauftragsverhältnisse

6.1. Definition von Unterauftragsverhältnissen

Unterauftragsverhältnisse im Sinne dieser Regelung sind Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen wie Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder Entsorgung von Datenträgern. Der Auftragnehmer muss auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers ergreifen.

6.2. Zustimmung des Auftraggebers

Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer bedarf der vorherigen Zustimmung des Auftraggebers in Textform. Alle bestehenden Unterauftragsverhältnisse sind in **Anlage 2** zu diesem Vertrag aufzuführen.

6.3. Auswahl und Kontrolle

Der Auftragnehmer wählt Unterauftragnehmer sorgfältig aus und prüft vor Beauftragung und regelmäßig während der Vertragsdauer, dass diese die vereinbarten Datenschutzmaßnahmen gemäß Art. 32 DS-GVO einhalten. Das Ergebnis der Kontrolle ist zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

6.4. Anwendung der Vertragsregelungen

Der Auftragnehmer stellt sicher, dass die vereinbarten Regelungen und Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

6.5. Auftragsverarbeitungsvertrag mit Unterauftragnehmer

Der Auftragnehmer schließt mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag, der den Anforderungen des Art. 28 DS-GVO entspricht. Der Unterauftragnehmer erhält dieselben Pflichten zum Schutz personenbezogener Daten wie der Auftragnehmer. Der Auftragsverarbeitungsvertrag wird dem Auftraggeber auf Anfrage in Kopie übermittelt.

6.6. Kontrollrechte

Der Auftragnehmer stellt sicher, dass die Kontrollrechte des Auftraggebers und der Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende vertragliche Regelungen getroffen werden.

6.7. Erbringung der Leistung außerhalb der EU/des EWR

Erbringt der Unterauftragnehmer die Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt für Nebenleistungen gemäß 6.1.

7. Kontrollrechte des Auftraggebers

7.1. Prüfungen durch Dritte

Der Auftraggeber kann die Prüfung durch einen benannten Dritten (Prüfer) durchführen lassen. Die Durchführung eines Audits ist mindestens fünf (5) Werktage im Voraus schriftlich anzukündigen. Der Auftraggeber hat keinen Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Kosteninformationen, Qualitätsprüfungen, Managementberichten oder anderen vertraulichen Daten, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind. Der Auftraggeber verpflichtet sich zur strikten Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers.

7.2. Auskunftspflicht des Auftragnehmers

Der Auftragnehmer stellt sicher, dass der Auftraggeber die Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überprüfen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3. Nachweis geeigneter Maßnahmen

Der Nachweis der Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch geeignete Maßnahmen erfolgen, darunter:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4. Kosten

Für die Wahrnehmung der Kontrollrechte fällt keine Vergütung an.

8. Weisungsbefugnis des Auftraggebers

8.1. Verarbeitung nach Weisung

Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten. Dies gilt insbesondere für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.

8.2. Bestätigung mündlicher Weisungen

Mündliche Weisungen sind vom Auftraggeber unverzüglich schriftlich oder in Textform zu bestätigen.

8.3. Information bei rechtswidrigen Weisungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung und Rückgabe von personenbezogenen Daten

9.1. Erstellung von Kopien

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt, ausgenommen sind Sicherheitskopien zur ordnungsgemäßen Datenverarbeitung und Daten zur Einhaltung gesetzlicher Aufbewahrungspflichten.

9.2. Rückgabe und Löschung der Daten

Nach Abschluss der vertraglich vereinbarten Arbeiten oder nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – händigt der Auftragnehmer sämtliche Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber aus oder vernichtet sie nach vorheriger Zustimmung datenschutzgerecht. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

9.3. Aufbewahrung von Dokumentationen

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, werden durch den Auftragnehmer entsprechend den gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt. Der Auftragnehmer kann diese Dokumentationen zur Entlastung dem Auftraggeber bei Vertragsende übergeben.

10. Vergütung

Die Vergütung des Auftragnehmers ergibt sich aus dem zugrundeliegenden Hauptvertrag. Für Maßnahmen nach diesem Vertrag steht dem Auftragnehmer keine zusätzliche Vergütung zu.

11. Haftung, Freistellung, Vertragsstrafe

11.1. Haftung des Auftragsverarbeiters

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die gesetzlichen Datenschutzbestimmungen. Dies gilt für Verstöße des Auftragsverarbeiters, seiner Mitarbeiter oder der von ihm beauftragten Personen bei der Erbringung der vertraglichen Leistung. Etwaige Haftungsbegrenzungen der Parteien aus dem Hauptvertrag finden keine Anwendung.

11.2. Ersatz von Schäden und Freistellung

Für den Ersatz von Schäden, die ein Betroffener aufgrund unzulässiger oder unrichtiger Datenverarbeitung im Rahmen des Auftragsverhältnisses geltend macht, ist der Verantwortliche

bzw. der Auftragsverarbeiter gem. Art. 82 DSGVO gegenüber dem Betroffenen verantwortlich. Der Auftragsverarbeiter stellt den Verantwortlichen im Innenverhältnis von allen Schadensersatzansprüchen frei, die aufgrund einer schuldhaften Verletzung der dem Auftragsverarbeiter auferlegten Pflichten oder der Nichtbeachtung rechtmäßig erteilter Weisungen des Verantwortlichen gegen den Verantwortlichen geltend gemacht werden. Der Auftragsverarbeiter trägt die Beweislast dafür, dass der Schaden nicht auf seiner Pflichtverletzung beruht und er diese nicht zu vertreten hat.

11.3. Vertragsstrafe

Verstößt der Auftragsverarbeiter gegen die Bestimmungen dieser Vereinbarung und/oder die geltenden Datenschutzbestimmungen, verpflichtet er sich zur Zahlung einer angemessenen Vertragsstrafe. Die Höhe der Vertragsstrafe bestimmt der Verantwortliche nach billigem Ermessen und unterliegt im Streitfall der Überprüfung durch das zuständige Gericht. Die Geltendmachung weitergehender Schadensersatzansprüche bleibt hiervon unberührt.

12. Sonstiges

- 12.1. Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor..
- 12.2. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind vom Auftragnehmer für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
- 12.3. Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen und ausdrücklich angeben, dass sie die vorliegenden Bestimmungen ändern und/oder ergänzen. Dies gilt auch für den Verzicht auf das Formerfordernis.
- 12.4. Sollte das Eigentum und/oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.
- 12.5. Die Einrede des Zurückbehaltungsrechts gemäß § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- 12.6. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

Anlage 1

Technische und organisatorische Maßnahmen (TOM)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Alarmanlage	<input type="checkbox"/> Schlüsselregelung / Liste
<input type="checkbox"/> Automatisches Zugangskontrollsystem	<input type="checkbox"/> Empfang / Rezeption / Pförtner
<input type="checkbox"/> Biometrische Zugangssperren	<input type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input type="checkbox"/> Chipkarten / Transpondersysteme	<input type="checkbox"/> Mitarbeiter- / Besucherausweise
<input type="checkbox"/> Manuelles Schließsystem	<input type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input type="checkbox"/> Sicherheitsschlösser	<input type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input type="checkbox"/> Schließsystem mit Codesperre	<input type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input type="checkbox"/> Absicherung der Gebäudeschächte	<input type="checkbox"/>
<input type="checkbox"/> Türen mit Knauf Außenseite	<input type="checkbox"/>
<input type="checkbox"/> Klingelanlage mit Kamera	<input type="checkbox"/>
<input type="checkbox"/> Videoüberwachung der Eingänge	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Login mit Benutzername + Passwort	<input type="checkbox"/> Verwalten von Benutzerberechtigungen
<input type="checkbox"/> Login mit biometrischen Daten	<input type="checkbox"/> Erstellen von Benutzerprofilen
<input type="checkbox"/> Anti-Viren-Software Server	<input type="checkbox"/> Zentrale Passwortvergabe
<input type="checkbox"/> Anti-Virus-Software Clients	<input type="checkbox"/> Richtlinie „Sicheres Passwort“
<input type="checkbox"/> Anti-Virus-Software mobile Geräte	<input type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input type="checkbox"/> Firewall	<input type="checkbox"/> Richtlinie „Clean desk“
<input type="checkbox"/> Intrusion Detection Systeme	<input type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input type="checkbox"/> Mobile Device Management	<input type="checkbox"/> Mobile Device Policy
<input type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	<input type="checkbox"/> Anleitung „Manuelle Desktopsperre“
<input type="checkbox"/> Verschlüsselung von Datenträgern	<input type="checkbox"/>
<input type="checkbox"/> Verschlüsselung Smartphones	<input type="checkbox"/>
<input type="checkbox"/> Gehäuseverriegelung	<input type="checkbox"/>
<input type="checkbox"/> BIOS Schutz (separates Passwort)	<input type="checkbox"/>
<input type="checkbox"/> Sperre externer Schnittstellen (USB)	<input type="checkbox"/>
<input type="checkbox"/> Automatische Desktopsperre	<input type="checkbox"/>

<input type="checkbox"/> Verschlüsselung von Notebooks / Tablet	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.3. 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Aktenschredder (mind. Stufe 3, cross cut)	<input type="checkbox"/> Einsatz Berechtigungskonzepte
<input type="checkbox"/> Externer Aktenvernichter (DIN 66399)	<input type="checkbox"/> Minimale Anzahl an Administratoren
<input type="checkbox"/> Physische Löschung von Datenträgern	<input type="checkbox"/> Datenschutztresor
<input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input type="checkbox"/> Steuerung über Berechtigungskonzept

<input type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger)	<input type="checkbox"/> Festlegung von Datenbankrechten
<input type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	<input type="checkbox"/> Datensätze sind mit Zweckattributen versehen
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	<input type="checkbox"/> Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

2. Integrität

2.1. 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> E-Mail-Verschlüsselung	<input type="checkbox"/> Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen

<input type="checkbox"/> Einsatz von VPN	<input type="checkbox"/> Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
<input type="checkbox"/> Protokollierung der Zugriffe und Abrufe	<input type="checkbox"/> Weitergabe in anonymisierter oder pseudonymisierter Form
<input type="checkbox"/> Sichere Transportbehälter	<input type="checkbox"/> Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
<input type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	<input type="checkbox"/> Persönliche Übergabe mit Protokoll
<input type="checkbox"/> Nutzung von Signaturverfahren	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

2.2. 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
<input type="checkbox"/>	<input type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
<input type="checkbox"/>	<input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
<input type="checkbox"/>	<input type="checkbox"/> Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input type="checkbox"/> Feuerlöscher Serverraum	<input type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input type="checkbox"/> Serverraumüberwachung Temperatur- und Feuchtigkeit	<input type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input type="checkbox"/> Serverraum klimatisiert	<input type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input type="checkbox"/> USV	<input type="checkbox"/> Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input type="checkbox"/> Existenz eines Notfallplans (z. B. BSI IT-Grundschutz 100-4)
<input type="checkbox"/> Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	<input type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten
<input type="checkbox"/> RAID System / Festplattenspiegelung	<input type="checkbox"/>
<input type="checkbox"/> Videoüberwachung Serverraum	<input type="checkbox"/>
<input type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Software-Lösungen für Datenschutz-Management im Einsatz	<input type="checkbox"/> Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
<input type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z. B. Wiki, Intranet ...)	<input type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
<input type="checkbox"/> Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	<input type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter: Mindestens jährlich
<input type="checkbox"/> Anderweitiges dokumentiertes Sicherheits-Konzept	<input type="checkbox"/> Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
<input type="checkbox"/> Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
<input type="checkbox"/>	<input type="checkbox"/> Die Organisation kommt den Informationspflichten nach
<input type="checkbox"/>	<input type="checkbox"/> Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen

<input type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input type="checkbox"/> Einbindung von <input type="checkbox"/> DSB und <input type="checkbox"/> ISB in Sicherheitsvorfälle und Datenschutzverletzungen
<input type="checkbox"/> Intrusion Detection System (IDS)	<input type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenschutzverletzungen z. B. via Ticketsystem
<input type="checkbox"/> Intrusion Prevention System (IPS)	<input type="checkbox"/> Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenschutzverletzungen
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	<input type="checkbox"/>
<input type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/>	<input type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
<input type="checkbox"/>	<input type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
<input type="checkbox"/>	<input type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
<input type="checkbox"/>	<input type="checkbox"/> Schriftliche Weisungen an den Auftragnehmer
<input type="checkbox"/>	<input type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
<input type="checkbox"/>	<input type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellopflicht
<input type="checkbox"/>	<input type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
<input type="checkbox"/>	<input type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
<input type="checkbox"/>	<input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input type="checkbox"/>	<input type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“). Dabei handelt es sich um die folgenden Unternehmen:

Unterauftragnehmer 1

- **Firma:** [Name des Unternehmens]
- **Rechtsform:** [Rechtsform des Unternehmens]
- **Kontaktdaten:** [Telefonnummer, E-Mail-Adresse]
- **Ladungsfähige Anschrift:** [Adresse]
- **Art der Leistung:** [Kurzbeschreibung der Leistung]

Unterauftragnehmer 2

- **Firma:** [Name des Unternehmens]
- **Rechtsform:** [Rechtsform des Unternehmens]
- **Kontaktdaten:** [Telefonnummer, E-Mail-Adresse]
- **Ladungsfähige Anschrift:** [Adresse]
- **Art der Leistung:** [Kurzbeschreibung der Leistung]

Unterauftragnehmer 3

- **Firma:** [Name des Unternehmens]
- **Rechtsform:** [Rechtsform des Unternehmens]
- **Kontaktdaten:** [Telefonnummer, E-Mail-Adresse]
- **Ladungsfähige Anschrift:** [Adresse]
- **Art der Leistung:** [Kurzbeschreibung der Leistung]

Ausgefüllt für den **AUFTRAGNEHMER** durch:

Name

Funktion

Rufnummer

E-Mail

Ort, Datum

(Unterschrift)

Vom **AUFTRAGGEBER** auszufüllen:

Geprüft am durch .

Ergebnis(se):

☐ Es besteht noch Klärungsbedarf zu

☐ Es besteht kein Klärungsbedarf mehr. Die Vereinbarung kann wie vorliegend abgeschlossen werden.

Mit der Unterschrift bestätigt der Mitarbeiter oder die Mitarbeiterin des DRK e.V. Generalsekretariats, dass eine Prüfung mit dem zuvor genannten Ergebnis durch den Datenschutzbeauftragten durchgeführt wurde.

Ort, Datum

(Unterschrift)