Vereinbarung zur Datenverarbeitung

Berlin Partner für Wirtschaft und Technologie GmbH,
vertreten durch den Geschäftsführer Dr. Stefan Franzke,
Fasanenstraße 85, 10623 Berlin

– im Folgenden **Berlin Partner (Auftraggeber)** genannt –

und

Klicken oder tippen Sie hier, um Text einzugeben.
vertreten durch den Klicken oder tippen Sie hier, um Text einzugeben. Klicken oder tippen Sie hier, um Text einzugeben.

– im Folgenden **Auftragnehmer/Dienstleister** genannt –

-im Folgenden gemeinsam die **Parteien** genannt

schließen nachfolgende Vereinbarung:

1. Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten vom Auftraggeber und -nehmer im Rahmen einer Verarbeitung personenbezogener Daten im Auftrag.
(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen personenbezogene Daten verarbeiten werden.
(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutzgrundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen
auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand, Dauer und Inhalte des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus der in Anlage 1 beigefügten Leistungsbeschreibung.
(2) Die Datenverarbeitung durch den Auftragnehmer erfolgt ausschließlich zum Zweck [Hier bitte den konkreten Zweck, z. B. Versand des Newsletters xy, Erstellung der Homepage …, Einladungsmanagement für … etc., angeben].

(3) Eine Kündigung dieser Vereinbarung kann durch beide Parteien mit einer Frist von drei Monaten zum Monatsende erfolgen. Der Auftrag endet – ohne dass es einer Kündigung bedarf – jedoch spätestens mit Ablauf des Kalenderjahres, in dem die in Anlage 1 beschriebenen
Leistungen abschließend erbracht worden sind. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.
(4) Die Art der personenbezogenen Daten sowie die Kategorien der durch die Verarbeitung betroffenen Personen ergeben sich aus der Leistungsbeschreibung [vgl. Anlage 1].

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. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 2].
(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 dieser 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 hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet der Auftragnehmer insbesondere die Einhaltung folgender Vorgaben:
a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Autragnehmer 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 diesem 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.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 2].
d) Der Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) 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.
f) 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.
g) 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.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 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) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
(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.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (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 ihrem Geschäftsbetrieb zu überzeugen.
(2) der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten vom Auftragnehmer nach Art. 28 DS-GVO 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.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B.

Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).
(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO 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 nicht auf ein Fehlverhalten vom Auftragnehmer 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.

Berlin, den Klicken oder tippen Sie, um ein Datum einzugeben.	Berlin, den Klicken oder tippen Sie, um ein Datum einzugeben.
Dr. Stefan Franzke Geschäftsführer der Berlin Partner für Wirtschaft und Technologie GmbH	Klicken oder tippen Sie hier, um Text einzugeben.

Anlage 1

Leistungsbeschreibung Auftragsdatenverarbeitung

A. Gegenstand des Auftrags

Klicken oder tippen Sie hier, um Text einzugeben.

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

Zutreffendes bitte ankreuzen

- ☐ Personenstammdaten (z.B. Name, Geschlecht, Altersgruppe)
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Sonstige: _____

C. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Zutreffendes bitte ankreuzen

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Sonstige:

_____

Anlage 2 (vom Auftragnehmer auszufüllen)

Bei den aufgeführten technischen und organisatorischen Maßnahmen handelt es sich um Beispiele: der Auftragnehmer soll hier die relevanten „anklicken“ und weitere ergänzen soweit vorhanden

Mustervorlage technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

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.

Stand: Mai 2019

Vertraulichkeit

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**
☐Alarmanlage	☐Schlüsselregelung / Liste
☐Automatisches Zugangskontrollsystem	☐Empfang / Rezeption / Pförtner
☐Biometrische Zugangssperren	☐Besucherbuch / Protokoll der Besucher
☐Chipkarten / Transpondersysteme	☐Mitarbeiter- / Besucherausweise
☐Manuelles Schließsystem	☐Besucher in Begleitung durch Mitarbeiter
☐Sicherheitsschlösser	☐Sorgfalt bei Auswahl des Wachpersonals
☐Schließsystem mit Codesperre	☐Sorgfalt bei Auswahl Reinigungsdienste
☐Absicherung der Gebäudeschächte	

☐Türen mit Knauf Außenseite	
☐Klingelanlage mit Kamera	
☐Videoüberwachung der Eingänge	
☐	☐
☐	☐

Weitere Maßnahmen bitte hier beschreiben:

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**
☐Login mit Benutzername + Passwort	☐Verwalten von Benutzerberechtigungen
☐Login mit biometrischen Daten	☐Erstellen von Benutzerprofilen
☐Anti-Viren-Software Server	☐Zentrale Passwortvergabe
☐Anti-Virus-Software Clients	☐Richtlinie „Sicheres Passwort“
☐Anti-Virus-Software mobile Geräte	☐Richtlinie „Löschen / Vernichten“
☐Firewall	☐Richtlinie „Clean desk“
☐Intrusion Detection Systeme	☐Allg. Richtlinie Datenschutz und / oder Sicherheit
☐Mobile Device Management	☐Mobile Device Policy

☐Einsatz VPN bei Remote-Zugriffen	☐Anleitung „Manuelle Desktopsperre“
☐Verschlüsselung von Datenträgern	
☐Verschlüsselung Smartphones	
☐Gehäuseverriegelung	
☐BIOS Schutz (separates Passwort)	
☐Sperre externer Schnittstellen (USB)	
☐Automatische Desktopsperre	
☐Verschlüsselung von Notebooks / Tablet	
☐	☐
☐	☐

Weitere Maßnahmen:

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**
☐Aktenschredder (mind. Stufe 3, cross cut)	☐Einsatz Berechtigungskonzepte
☐Externer Aktenvernichter (DIN 32757)	☐Minimale Anzahl an Administratoren
☐Physische Löschung von Datenträgern	☐Datenschutztresor

☐Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐Verwaltung Benutzerrechte durch Administratoren
☐	☐
☐	☐

Weitere Maßnahmen:

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**
☐Trennung von Produktiv- und Test- umgebung	☐Steuerung über Berechtigungskonzept
☐Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐Festlegung von Datenbankrechten
☐Mandantenfähigkeit relevanter Anwendungen	☐Datensätze sind mit Zweckattributen versehen
☐	☐
☐	☐

Weitere Maßnahmen:

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 technichen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☐Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

☐	☐
☐	☐

Weitere Maßnahmen:

Integrität

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**
☐Email-Verschlüsselung	☐Dokumentation der Datenempfänger sowie der Dauer der geplanten Über- lassung bzw. der Löschfristen
☐Einsatz von VPN	☐Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐Protokollierung der Zugriffe und Abrufe	☐Weitergabe in anonymisierter oder pseudonymisierter Form
☐Sichere Transportbehälter	☐Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
☐Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐Persönliche Übergabe mit Protokoll
☐Nutzung von Signaturverfahren	
☐	☐
☐	☐

Weitere Maßnahmen:

Eingangskontrolle
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**
☐Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐Manuelle oder automatisierte Kontrolle der Protokolle	☐Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	☐Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☐Aufbewahrung von Formularen, von denen Daten in automatisierte Verar- beitungen übernommen wurden
	☐Klare Zuständigkeiten für Löschungen
☐	☐
☐	☐

Weitere Maßnahmen:

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

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

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

Weitere Maßnahmen:

<u>Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung</u>

Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☐Software-Lösungen für Datenschutz-Management im Einsatz	☐Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
☐Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	☐Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☐Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
☐Anderweitiges dokumentiertes Sicherheitskonzept	☐Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
☐Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☐Die Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)
	☐Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☐Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐
☐	☐

Weitere Maßnahmen:

Incident-Response-Management
Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen

☐Einsatz von Firewall und regelmäßige Aktualisierung	☐Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☐Einsatz von Spamfilter und regelmäßige Aktualisierung	☐Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☐Einsatz von Virenscanner und regelmäßige Aktualisierung	☐Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☐Intrusion Detection System (IDS)	☐Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☐Intrusion Prevention System (IPS)	☐Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☐	☐
☐	☐

Weitere Maßnahmen:

Datenschutzfreundliche Voreinstellungen
Privacy by design / Privacy by default

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
☐Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	
☐	☐
☐	☐

Weitere Maßnahmen:

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.

☐ Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.

Falls Sie Subunternehmer einsetzen, bitte noch folgende Tabelle befüllen:

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☐Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaß- nahmen und deren Dokumentation
☐	☐Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☐	☐Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
☐	☐Schriftliche Weisungen an den Auftragnehmer
☐	☐Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☐Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐	☐Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☐Regelung zum Einsatz weiterer Sub- unternehmer
☐	☐Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐	☐Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
☐	☐
☐	☐

Weitere Maßnahmen:

Ausgefüllt für die Organisation durch

Name Funktion Rufnummer Email

Ort, Datum