Dienstanweisung für den organisatorischen und technischen Datenschutz bei der Stadtverwaltung Speyer vom 9.5.2019

SPEYER

I n h a l t s v e r z e i c h n i s :

TEIL D: Verarbeitung von papiergebundenen Akten

TEIL E: Schlussbestimmungen

Anlagen:

1) **Anlage 1 zu § 6:**
   Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)

2) **Anlage 2 zu § 13:**
   Muster einer Beschreibung einer Verarbeitungstätigkeit nach Art. 30 Abs. 1 DSGVO

3) **Anlage 3 zu § 15:**
   Muster/Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

Dienstanweisung

für den organisatorischen und technischen

Datenschutz bei der Stadtverwaltung Speyer

vom 9.5.2019

TEIL A: Allgemeines

§ 1 Geltungsbereich

Diese Dienstanweisung gilt für die Verarbeitung personenbezogener Daten durch alle Organisationseinheiten der Stadtverwaltung Speyer. Soweit weitere oder von den nachfolgenden Bestimmungen abweichende Maßnahmen für einzelne Anwendungen erforderlich sind, werden diese für die jeweilige Anwendung schriftlich festgelegt. Die Angelegenheiten zum Thema Datenschutz im schulischen Umfeld werden für das Personal der Schulsekretariate auf die Schulleitungen übertragen.

Die Nutzung von Internet und E-Mail durch die Mitarbeiter/innen der Stadtverwaltung ist in der Dienstanweisung „Elektronische Medien“ in der aktuell gültigen Fassung geregelt. Diese und alle sonstigen zu speziellen Inhalten mit Datenschutzbezug getroffenen Dienstanweisungen bleiben von der vorliegenden Dienstanweisung unberührt. Bestehende und künftige verwaltungsinterne Regelungen, soweit sie den Datenschutz betreffen, sind dieser Dienstanweisung anzupassen.

§ 2 Begriffsbestimmungen

Der Begriff “Personenbezogene Daten” bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, z.B. ein/e Kollege/in oder ein/e Kunde/in. Ein Mensch ist identifizierbar, wenn er/sie direkt oder indirekt (insbesondere mittels einer Kennung wie Name, Standortdaten, Nummer oder Merkmalen) identifiziert werden kann. Zu den personenbezogenen Daten gehören somit z.B. Adresse, Telefonnummer, Geburtsdatum, Gehalt, Vermögen, Fotos, Beruf, Erscheinungsbild etc.

Der Begriff “Verarbeitung” bezeichnet jeden Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben (Beschaffen), das Erfassen und Speichern, die Organisation und das Ordnen, die Anpassung oder Veränderung, das Auslesen und Abfragen, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung sowie die Verwendung.

TEIL B: Organisatorischer Datenschutz

1. Datenschutzrechtliche Zuständigkeiten

§ 3 Oberbürgermeister/in

(1) Der/die Oberbürgermeister/in stellt mit Unterstützung der nachfolgend genannten Organisationseinheiten sicher, dass die Verarbeitung personenbezogener Daten im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt.

(2) Der/die Oberbürgermeister/in benennt eine/n behördliche/n Datenschutzbeauftragte/n und deren/dessen Vertretung, soweit gesetzlich oder in dieser Dienstanweisung nicht anderes bestimmt ist.

§ 4 Hauptverwaltung

Die Hauptverwaltung erarbeitet im Benehmen mit der/dem behördlichen Datenschutzbeauftragten und der EDV-Abteilung geeignete Datenschutzvorkehrungen nach Art. 24 Abs. 2 DSGVO. Hierzu gehören insbesondere Datenschutz-Richtlinien und fachverfahrensspezifische Anweisungen an die Beschäftigten.

§ 5 EDV-Abteilung

Die EDV-Abteilung legt in Abstimmung mit den nach §§ 3 und 4 zuständigen Organisationseinheiten

a) geeignete technische Maßnahmen zum Schutz der zu verarbeitenden Daten nach Art. 24 Abs. 1, Art. 25 und Art. 32 DSGVO,

b) angemessene und spezifische Maßnahmen zum Schutz besonderer Kategorien personenbezogener Daten nach § 19 LDatSchG,

c) ggf. geeignete Maßnahmen nach § 19 Abs. 3 LDatSchG

fest.

§ 6 Verpflichtung auf das Datengeheimnis

Mitarbeiter/innen sowie sonstige Personen (u.a. Gastauszubildende, Praktikanten, etc.), die dienstlichen Zugang zu personenbezogenen Daten haben, sind nach § 8 Landesdatenschutzgesetz unter Verwendung des als Anlage 1 angefügten Vordrucks vor der Arbeitsaufnahme auf die Einhaltung des Datengeheimnisses zu verpflichten. Die Verpflichtung von Mitarbeiter/innen erfolgt jeweils durch die Organisationseinheit, welche die Einstellung veranlasst (Personalabteilung, Zentrales Gebäudemanagement). Die Verpflichtung von sonstigen Personen erfolgt durch die jeweilige Fachabteilung, welcher die Person zugeordnet ist.

§ 7 Fachbereiche und Stabsstellen

(1) Alle Fachbereiche und Stabsstellen sind in ihrem Zuständigkeitsbereich für die Beachtung der datenschutzrechtlichen Vorschriften verantwortlich.

(2) Im Benehmen mit der/dem behördlichen Datenschutzbeauftragten stellen die Organisationseinheiten für ihren Zuständigkeitsbereich sicher, dass die Rechte der betroffenen Personen nach Art. 12, Art. 15 und Art. 22 DSGVO sowie die Informationspflichten nach Art. 13 und Art. 14 DSGVO erfüllt werden.

§ 8 Behördliche/r Datenschutzbeauftragte/r

	Die Aufgaben des/der Datenschutzbeauftragten umfassen:	
	I. Gesetzliche Aufgaben	**Rechts-grundlage**
	1. Unterrichtung und Beratung der/des Verantwortlichen oder des Auftragsverarbeiters und der Mitarbeiter/innen, die Verarbeitungen	Art. 39 Abs. 1 a

	durchführen, hinsichtlich ihrer Pflichten, die sich aus dem Datenschutzrecht (DSGVO sowie allgemeine und bereichsspezifische nationale Datenschutzregelungen) ergeben	DSGVO
	2. Überwachung der Einhaltung der DSGVO und nationaler Datenschutzvorschriften sowie der Strategien der/des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, die Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter/innen und diesbezügliche Überprüfungen	Art. 39 Abs. 1 b DSGVO
	3. Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO	Art. 39 Abs. 1 c DSGVO
	4. Zusammenarbeit mit der Aufsichtsbehörde	Art. 39 Abs. 1 d DSGVO
	5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO und ggf. Beratung zu allen sonstigen Fragen	Art. 39 Abs. 1 e DSGVO
	6. Beratung betroffener Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechts gemäß DSGVO im Zusammenhang stehende Fragen	Art. 38 Abs. 4 DSGVO
	7. Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden	§ 36 LDSG
	8. Stellungnahme vor dem Einsatz geplanter Videoüberwachungen, insbesondere hinsichtlich Zweck, räumlicher Ausdehnung, Dauer der Videoüberwachung, betroffenem Personenkreis, vorgesehener Maßnahmen zur Kenntlichmachung und vorgesehener Auswertungen	§ 21 LDSG
	9. Erstellen von Berichten und Meldungen an die Behördenleitung	Art. 38 Abs. 3 S. 3 DSGVO
	10. Regelmäßige eigene Fortbildung zum Datenschutz	

Ergänzend zu den durch Art. 39 Abs. 1 DSGVO sowie § 39 LDatSchG zugewiesenen Aufgaben werden der/dem behördlichen Datenschutzbeauftragten die nachfolgenden Aufgaben übertragen:

- Koordinierung der Erfüllung der Rechte der betroffenen Personen nach Art. 12, Art. 15 bis 22 DSGVO durch die jeweilige Fachabteilung einschließlich Beteiligung bei deren abschließenden Entscheidungen über Betroffenenrechte
- Begleitung der Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 Abs. 2 DSGVO
- Organisation der Schulung von Mitarbeitern/Mitarbeiterinnen
- Umsetzung der Meldung bzw. Benachrichtigung bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO

- Koordinierung der Führung des Verarbeitungsverzeichnisses durch die Fachabteilungen nach Art. 30 DSGVO

2. Zusammenarbeit

§ 9 Zusammenarbeit und gegenseitige Information

(1) Die Hauptverwaltung, die EDV-Abteilung und die/der behördliche Datenschutzbeauftragte arbeiten zur Gewährleistung des Datenschutzes vertrauensvoll zusammen und informieren sich gegenseitig. Hierzu schaffen sie geeignete Verfahren der kontinuierlichen Zusammenarbeit. Sie unterrichten die Behördenleitung über alle wesentlichen Vorgänge.

(2) Jede/r Mitarbeiter/in meldet ihrem/seinem jeweiligen Vorgesetzten unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen. Die Fachabteilungen informieren unverzüglich die/den behördlichen Datenschutzbeauftragten über den Verstoß.

3. Datenschutzrechtliche Ablauforganisation

Abschnitt 1: Allgemeine Grundsätze zur Gewährleistung des Datenschutzes

§ 10 Information der Mitarbeiter/innen

Die Mitarbeiter/innen sind auf geeignete Art und Weise für den Umgang mit personenbezogenen Daten zu sensibilisieren.

§ 11 Beteiligung der/des behördlichen Datenschutzbeauftragten

(1) Die/der behördliche Datenschutzbeauftragte wird frühzeitig in alle wesentlichen Datenschutzfragen eingebunden und von der Hauptverwaltung, der EDV-Abteilung, den Abteilungsleitungen sowie allen MitarbeiterInnen bei der Erfüllung der Aufgaben unterstützt.

(2) Ihr/ihm ist vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme zu geben.

(3) Vor dem Einsatz einer Videoüberwachung sind der/dem behördlichen Datenschutzbeauftragten der Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, der betroffene Personenkreis, die Maßnahmen nach § 21 LDatSchG und die vorgesehenen Auswertungen mitzuteilen. Ihm ist Gelegenheit zur Stellungnahme zu geben.

(4) Die/der behördliche Datenschutzbeauftragte ist im Vorfeld von Vergabeverfahren und neuer Fachverfahren sowie vor der Beschaffung von IT-Hard- und Software zu beteiligen, wenn datenschutzrechtlich bedeutsame Anschaffungen geplant werden.

(5) Vor Abschluss eines Auftragsverarbeitungsvertrages ist der/dem behördlichen Datenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben (siehe § 15).

§ 12 Datenschutzbericht

Die/der behördliche Datenschutzbeauftragte erstellt mindestens alle zwei Jahre einen Bericht zum Datenschutz. In diesem sind die in der Stadtverwaltung zur Gewährleistung des Datenschutzes eingesetzten technischen und organisatorischen

Maßnahmen darzustellen sowie ggf. festgestellte Datenschutzverstöße und Schutzlücken aufzuführen. Die Ergebnisse des Berichts werden mit der Behördenleitung und den zuständigen Fachabteilungen erörtert und Verbesserungsmöglichkeiten geprüft. Der Bericht ist nicht öffentlich.

§ 13 Gewährleistung der Richtigkeit und Vollständigkeit des Verarbeitungsverzeichnisses

(1) Für jedes automatisierte Fachverfahren ist durch die fachlich zuständige Organisationseinheit eine Verfahrensbeschreibung zu erstellen und fortzuschreiben. Das Verarbeitungsverzeichnis wird von den jeweiligen Fachabteilungen geführt. Die fachlich zuständigen Organisationseinheiten informieren den/die behördliche/n Datenschutzbeauftragte/n unaufgefordert über neu aufgenommene Verarbeitungstätigkeiten sowie wesentliche Änderungen bereits gemeldeter Verarbeitungstätigkeiten. Der/dem behördlichen Datenschutzbeauftragten ist Zugriff auf das Verarbeitungsverzeichnis zu gewähren.

(2) Für die Führung des Verarbeitungsverzeichnisses ist der als Anlage 2 beigefügte Vordruck zu verwenden.

Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen

§ 14 Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO

(1) Im Fall einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO informiert die jeweilige Organisationseinheit, der die Datenschutzverletzung bekannt geworden ist, unverzüglich die/den behördlichen Datenschutzbeauftragten.

(2) Soweit der/dem Oberbürgermeister/in, der Hauptverwaltung und der EDV-Abteilung der Verstoß noch nicht bekannt ist, unterrichtet die/der behördliche Datenschutzbeauftragte diese. Sie/er teilt ihnen dabei ihre/seine Einschätzung mit, ob eine Meldepflicht nach Art. 33 DSGVO oder eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. Die Einschätzung ist schriftlich zu begründen.

(3) Der/die Oberbürgermeister/in meldet die Verletzung des Schutzes personenbezogener Daten unverzüglich der/dem Landesbeauftragten für Datenschutz und Informationsfreiheit mit dem nach Art. 33 DSGVO vorgegebenen Mindestinhalt, möglichst innerhalb einer Frist von 72 Stunden. Ist eine Meldung innerhalb von 72 Stunden nicht möglich, sind die Gründe hierfür zu dokumentieren und die Meldung unverzüglich nachzuholen. Die Meldung unterbleibt, wenn die Hauptverwaltung und die EDV-Abteilung unter Berücksichtigung der Einschätzung des behördlichen Datenschutzbeauftragten nach Abs. 2 der Auffassung sind, dass die Voraussetzungen des Art. 33 DSGVO nicht vorliegen. Die Gründe hierfür sind zu dokumentieren. Wenn Daten von oder an die/den Verantwortlichen eines anderen Mitgliedsstaates übermittelt wurden, sind im Anwendungsbereich der §§ 26 - 36 LDatSchG die Informationen nach Art. 33 Abs. 3 DSGVO unverzüglich auch an diese/n zu melden.

(4) Die Hauptverwaltung und die EDV-Abteilung entscheiden auf der Grundlage der Einschätzung der/des behördlichen Datenschutzbeauftragten nach Abs. 2, ob eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat und somit eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. Die Benachrichtigung der betroffenen Person erfolgt unverzüglich durch die für die

Umsetzung der Benachrichtigung zuständigen Organisationseinheit. Unterbleibt eine Benachrichtigung nach Art. 34 DSGVO, sind die Gründe hierfür zu dokumentieren.

(5) Nach Bekanntwerden des Verstoßes leiten die Hauptverwaltung und die EDV-Abteilung in Abstimmung mit der/dem behördlichen Datenschutzbeauftragten unverzüglich Abhilfemaßnahmen ein.

§ 15 Auftragsverarbeitung

Die Verarbeitung personenbezogener Daten im Auftrag durch andere Firmen/Personen oder Stellen ist durch einen Auftragsverarbeitungsvertrag zu regeln. Die Fachabteilung prüft vor Abschluss eines Vertrages über die Auftragsverarbeitung, ob der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass

- geeignete technische und organisatorische Maßnahmen durchgeführt werden
- die Verarbeitung im Einklang mit den Anforderungen der DSGVO und den zu ihrer Ergänzung erlassenen europäischen, bundes- und landesrechtlichen Regelungen erfolgt und
- der Schutz der Rechte der betroffenen Person gewährleistet wird.

Hierzu lässt sich die Fachabteilung entsprechende Nachweise / Zertifikate vorlegen und holt die Stellungnahme der/des behördlichen Datenschutzbeauftragten sowie der EDV-Abteilung ein. Bei der Vertragsgestaltung ist das als Anlage 3 beigefügte Muster zu Grunde zu legen. Weiterhin ist zu prüfen, inwieweit hierfür spezialgesetzliche Regelungen bestehen (z.B. § 80 SGB X).

§ 16 Vertrauliche Meldung von Datenschutzverstößen nach § 65 Landesdatenschutzgesetz Rheinland-Pfalz

Erlangt ein/e Mitarbeiter/in von einem Datenschutzverstoß Kenntnis, kann er/sie sich, ohne Einhaltung des Dienstweges unmittelbar an den/die behördliche/n Datenschutzbeauftragte/n wenden, wenn er erkennen sollte, dass die interne Aufarbeitung des Datenschutzverstoßes nicht oder nicht ausreichend stattfindet. Die/der behördliche Datenschutzbeauftragte behandelt die Meldung vertraulich. Sie/er darf Tatsachen, die ihr/ihm in Ausübung ihrer/seiner Funktion anvertraut wurden, und die Identität der mitteilenden Person nicht ohne dessen Einverständnis offenbaren.

TEIL C: Technischer Datenschutz

§ 17 Auswahl, Einsatz und Entwicklung von automatisierten Verfahren; Datensicherung

1. Bei der Auswahl und Entwicklung von automatisierten Verfahren ist darauf zu achten, dass bei ihrer Anwendung der Umfang der zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten auf ein Minimum beschränkt wird (Grundsatz der Datenvermeidung und der Datensparsamkeit)

2. Alle eingesetzten Verfahren bedürfen der schriftlichen Freigabe durch die EDV-Abteilung.

3. Änderungen an der Konfiguration der Systemumgebung sind grundsätzlich nur durch die EDV-Abteilung zulässig.

4. Datenbestände sind in regelmäßigen Zeitabständen so zu sichern, dass sie im Fall des Verlust oder der Zerstörung mit vertretbarem Aufwand wiederhergestellt werden können.

§ 18 Zutritt zu Gebäuden und Räumen

1. Dienstgebäude, in denen Serviceleistungen für den Bürger angeboten werden, sind während der Dienststunden grundsätzlich geöffnet. Nicht zugänglich für unbefugte Personen sind Gebäude bzw. Räumlichkeiten, in denen Registraturen, Archive sowie Systeme für die IT-Infrastruktur (z.B. Räume für Server, Drucker, etc.) untergebracht sind.

   Die Ausgabe von Schlüsseln/Transpondern ist schriftlich oder mittels Datei zu dokumentieren. Bei Ausscheiden aus dem Bereich oder der Abteilung sind die Schlüssel für Gebäude und Büro zurückzugeben.

   Für Gebäude mit elektronischer Schließanlage gilt die entsprechende Dienstvereinbarung.

   Zu den Räumen, in denen sich zentrale Einrichtungen der Datenverarbeitung befinden, dürfen nur ausdrücklich berechtigte Mitarbeiter/innen Zutritt haben. Der Zutritt darf nur durch entsprechende Schließ- oder Chipkartensysteme möglich sein.

   Reinigungs-, Wartungs- und ähnliche Aufgaben dürfen nur in Anwesenheit autorisierter Mitarbeiter/innen durchgeführt werden. Serverräume sind grundsätzlich mit einer Gefahrenmeldeanlage, Sicherheitstüren sowie einer Klimatisierung auszustatten.

2. Räume, in denen sich Datenverarbeitungsgeräte oder Datenträger befinden, sind bei Abwesenheit grundsätzlich zu verschließen. Bei Unterbrechung oder Beendigung der Bildschirmarbeit und Verlassen der Diensträume ist die unbefugte Nutzung durch Sperrung oder Abmeldung der Geräte zu verhindern.

   Nach Dienstschluss sind Zimmer-/Bürotüren zu verschließen. Unabhängig davon sind Schränke, die zentrale Einrichtungen der Informationstechnik (z.B. Netzwerkserver, DFÜ-Anschlüsse) enthalten, immer zu verschließen.

3. Bildschirmgeräte sind so aufzustellen, dass sie von Unbefugten nicht eingesehen werden können.

4. Fremde (z.B. Handwerker, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein. Ist eine ständige Beaufsichtigung nicht möglich (z.B. bei Reinigungspersonal), müssen schützenswerte Unterlagen weggeschlossen werden.

§ 19 Einsatz von dienstlicher Hard- und Software

Es dürfen grundsätzlich nur die Hard- und Softwarekomponenten eingesetzt werden, die über die EDV-Abteilung beschafft wurden und den städtischen EDV-Standards entsprechen.

Hierdurch soll gewährleistet werden, dass nur Systeme und Programme zum Einsatz kommen, die von der EDV-Abteilung vorab auf ihre Verträglichkeit mit der eingesetzten Systemumgebung überprüft worden sind. Private Hard- und Software darf nicht am Arbeitsplatz benutzt werden.

§ 20 Zugriff auf dienstliche EDV-Systeme

1. Für autorisierte Mitarbeiter/innen ist eine Benutzerkennung einzurichten und ein Anfangspasswort zuzuweisen. Dieses ist bei der ersten Anmeldung durch den/die

Anwender/in zu ändern. Sofern möglich, ist diese Änderung automatisiert vorzugeben.

Der Zugang zum dienstlich genutzten PC erfolgt mittels User-ID und Passwort. Die folgenden Hinweise zum Erstellen eines sicheren Passwortes sind zu beachten:

- Das Passwort sollte leicht zu merken, für andere jedoch schwer zu erraten sein. Es sollten keine Trivialpasswörter wie Namen, Geburtstage, Telefonnummern, Urlaubsziele verwendet werden. Auch gängige Zeichenfolgen (12345, abcde, etc.) bieten keinen wirksamen Schutz.
- Das Passwort sollte mindestens 8 Zeichen lang sein und aus Buchstaben, Zahlen und Sonderzeichen bestehen. Gestaltungsmöglichkeiten wie Zeichenmischung und Verfremdung (z.B. *zerberus* wird zu *z§rb§r§s* oder *z1rb2r3s*) oder die Mnemotechnik (*Einmal ist keinmal!* wird zu *1x=k1x!*) sollten genutzt werden.

Nach längstens drei Monaten ist das Passwort durch den Nutzer selbst zu ändern. Erfolgt keine Änderung, ist sicherzustellen, dass die Benutzerkennung gesperrt wird.

2. Generell ist die Weitergabe der Passwörter an Dritte nicht zulässig.

3. Besteht der Verdacht, dass Unbefugte Kenntnis von einem Passwort erhalten haben, ist unverzüglich ein neues Passwort einzurichten.

4. Passwörter dürfen nicht unverschlüsselt in Dateien abgelegt werden.

5. Sämtliche schriftliche Unterlagen, aus denen Rückschlüsse auf Zugangsmöglichkeiten zum System (z.B. Benutzerkennung, Passwort) gezogen werden können, sind sorgfältig und für Unbefugte unzugänglich aufzubewahren.

6. Bei Nichtbenutzung des PC erfolgt nach 90 Sekunden eine automatische Sperrung durch einen passwortgeschützten Sperrbildschirm. Diese Funktion wird zentral durch die EDV-Abteilung eingerichtet.

§ 21 Beschränkung von Zugriffsmöglichkeiten; Zugriffsrechteverwaltung

1. Zugriffsmöglichkeiten auf personenbezogene Daten sind auf den für die Aufgabenerfüllung erforderlichen Umfang zu beschränken. Die Abteilungsleitung der fachlich zuständigen Organisationseinheit bestimmt, welche Mitarbeiter/innen in welchem Umfang autorisiert sind, Daten zu verarbeiten.

2. Personenbezogene Daten, die gegenüber der Systembetreuung und Personen mit erweiterten Zugriffsrechten vertraulich zu halten sind (z.B. Personal-, Sozial- oder Gesundheitsdaten) sind auf mobilen Datenverarbeitungssystemen in angemessener Form kryptografisch zu verschlüsseln. Die notwendigen technischen Lösungen sind durch die EDV-Abteilung zur Verfügung zu stellen.

3. Multifunktionsgeräte (u.a. Kopierer, Scanner), die sich in öffentlich zugänglichen Bereichen befinden, sind mit einem PIN geschützten Zugang zu versehen, d.h. Druckausgaben können nur durch die hierzu berechtigten Mitarbeiter/innen vorgenommen werden.

§ 22 Protokollierung

1. Die Nutzung von Datenverarbeitungssystemen ist, soweit technisch möglich, mit den Angaben über die Benutzer, Zeitpunkt der An- und Abmeldung sowie fehlerhaften Zugriffsversuchen zu protokollieren. Darüber hinaus gehende Protokollierungen zur Verarbeitung personenbezogener Daten (Eingabe, Veränderung, Abfrage, Auswertung und Löschung) sind in Absprache mit den zuständigen Organisationseinheiten festzulegen. Die/der behördliche Datenschutzbeauftragte und der Personalrat sind zu beteiligen.

2. Die Protokolldaten dürfen gemäß § 64 LDSG ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung, die Eigenüberwachung, die Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet werden.

3. Protokolle, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen erstellt werden, dürfen nur von der Leitung der EDV-Abteilung gemeinsam mit der/dem behördlichen Datenschutzbeauftragten eingesehen werden. Weitergehende gesetzliche Befugnisse (z.B. Auskunfts- und Einsichtsrechte des Landesbeauftragten für den Datenschutz sowie Strafverfolgungsbehörden oder Beteiligungsrechte der Personalvertretung) bleiben unberührt.

§ 23 Gewährleistung der Zweckbindung

1. Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können. Dem ist grundsätzlich dadurch zu entsprechen, dass die Verarbeitung in getrennten Verfahren erfolgt. Ist dies nicht möglich oder zweckdienlich, sind die betroffenen Daten in verschiedenen Dateien zu speichern.

2. Soweit die gemeinsame Speicherung in einer Datei technisch bedingt oder aus sachlichen Gründen geboten ist, sind die Dateien so zu kennzeichnen, dass eine getrennte Verarbeitung möglich ist (Sortiermerkmale, Kennziffern, o.ä.)

§ 24 Empfang, Versand und Weitergabe

1. Beim Versand von personenbezogenen Daten ist eine ausreichend sichere Versandform zu wählen. Personenbezogene Daten dürfen nur über besonders gesicherte Netze oder mit besonderen Verfahren der Dienststelle übermittelt werden (z.B. rlp-Netz). Die unverschlüsselte Übermittlung personenbezogener Daten per E-Mail über das Internet ist rechtswidrig, da eine unbefugte Kenntnisnahme Dritter nicht ausgeschlossen ist. Personenbezogene Daten, die per E-Mail versendet oder empfangen werden, sind immer angemessen zu verschlüsseln. Die Art und Auswahl der notwendigen Verschlüsselungsverfahren bestimmt die EDV-Abteilung.

2. Die Weitergabe von Datenträgern innerhalb der Verwaltung hat persönlich oder in einem verschlossenen Umschlag mit dem Hinweis „persönlich“ zu erfolgen.

§ 25 Speicherung von Daten und Datensicherungsmaßnahmen

1. Daten sind grundsätzlich auf den vernetzten Serversystemen die durch die EDV-Abteilung eingerichtet werden, zu speichern. Die Datensicherung erfolgt durch die EDV-Abteilung.

2. Die Nutzung von Massenspeichern, die an die PC-Systeme der Verwaltung angeschlossen werden, birgt ein hohes Risiko eine Schadsoftware einzuschleusen. Die Nutzung dieser Geräte an den städtischen PC wird aus diesem Grund eingeschränkt, d.h. die Schnittstellen der PC sind durch die EDV-Abteilung zu sperren. Die Fachbereiche haben die Möglichkeit externe Datenträger durch die EDV-Abteilung einzuspielen oder sich einen Onlinespeicher (Cloud) von der EDV-Abteilung zur Verfügung stellen zu lassen.

3. Nicht mehr benötigte Datenträger sind zu löschen oder ordnungsgemäß zu entsorgen. Sie sind zum Zwecke der Entsorgung an die EDV-Abteilung zu übergeben. Bei der sicheren Löschung oder Vernichtung der Datenträger ist die diesbezüglich aktuell gültige DIN-Norm zu beachten.

4. Grundsätzlich findet ein Datenträgeraustausch nur über vernetzte IT-Systeme statt, um Schadensmöglichkeiten (z.B. Datenverlust, Beschädigung, Virenbefall) auszuschließen. Soweit dies nicht möglich ist, gelten folgende Regelungen:

   - Wechseldatenträger (u.a. USB-Sticks) werden vor dem Zugriff unbefugter Personen durch Verschlüsselung geschützt. Die Mitnahme solche Datenträger außerhalb des Dienstgebäudes ist nur in begründeten Ausnahmefällen (z.B. Dienstreise) erlaubt.
   - Personenbezogene Daten sind zu verschlüsseln
   - Vor bzw. nach einem Datenträgeraustausch ist eine Überprüfung der aus- bzw. eingehenden Daten durch einen Virenscanner vorzunehmen.

§ 26 Löschung, Sperrung und Archivierung

1. Für jedes Verfahren ist von der fachlich zuständigen Organisationseinheit, in der das Verfahren eingesetzt wird, ein Zeitpunkt festzulegen, nach dessen Ablauf die personenbezogenen Daten nach den datenschutzrechtlichen Vorschriften oder einer vorrangigen spezialgesetzlichen Regelung enthaltenen Vorgaben zu löschen oder zu sperren sind. Die EDV-Abteilung ist hiervon zu unterrichten.

2. Die Verantwortung für die Löschung oder Sperrung der Daten liegt bei der fachlich zuständigen Organisationseinheit, in der das Verfahren eingesetzt wird. Diese entscheidet in Abstimmung mit der EDV-Abteilung über das konkrete Verfahren. Die allgemeine Anbietungspflicht nach § 7 Abs. 1 Landesarchivgesetz bleibt hiervon unberührt.

3. Personenbezogene Daten in abgeschlossenen Fällen, die für die laufende Bearbeitung nicht mehr benötigt werden, sind durch die Übernahme in einen gesonderten Datenbestand oder die Vergabe von Zugriffsrechten so zu sichern, dass ein Zugriff nur in begründeten Fällen möglich ist (interne Archivierung).

§ 27 Wartung

1. Wartungsarbeiten an Datenverarbeitungsgeräten dürfen nur in Anwesenheit einer/eines verantwortlichen Mitarbeiterin/Mitarbeiters durchgeführt werden.

2. Auch für das Wartungspersonal ist eine Benutzerkennung mit Passwort zu vergeben. Es ist sicherzustellen, dass diese Kennung nur für Wartungsfälle benutzt werden kann. Die Inanspruchnahme ist zu dokumentieren (z.B. Eintragung in Logbuch, automatische Protokollierung).

3. Für die Einrichtung eines Verfahrens zur Fernwartung trifft die EDV-Abteilung im Hinblick auf dessen genaue Ausgestaltung näheren Bestimmungen. Die/der behördliche Datenschutzbeauftragte ist zu beteiligen.

§ 28 Einsatz von tragbaren IT-Systemen

Der Einsatz von Laptop, Notebook, Tablet-PC, Smartphones und Handys stellt an die Datensicherheit und den Datenschutz erhöhte Anforderungen, da diese Geräte durch ihre hohe Mobilität leicht beschädigt oder entwendet werden und somit auch wichtige Daten verloren gehen können. Folgende Punkte sind zu beachten:

- Die Geräte sind zwingend mit einem PIN/Passwort zu schützen. Eine Nutzung ohne die entsprechenden Zugangsdaten ist ausgeschlossen.
- Eine sichere Aufbewahrung verhindert den Diebstahl (z.B. in einem verschließbaren Fach oder Schrank). Transportable PC können auch durch ein Schloss gesichert werden, das mit einem fest verankerten Punkt verbunden ist.
- Wird das tragbare Gerät in einem Büroraum genutzt, so ist dieser Raum auch bei kurzzeitigem Verlassen zu verschließen.
- Die Geräte sind vor unbefugter Nutzung durch Nicht-Mitarbeiter/innen (z.B. Familienmitglieder) zu schützen.
- Es dürfen keine Hard- oder Softwareveränderungen an den Geräten ohne das Einverständnis der EDV-Abteilung vorgenommen werden.
- Personenbezogene bzw. vertrauliche Daten dürfen nicht lokal auf tragbaren IT-Systemen gespeichert werden. Überflüssige bzw. nicht mehr benötigte Daten sind regelmäßig zu löschen.
- Es muss geregelt sein, wie die Entsorgung der Geräte erfolgt, so dass sichergestellt ist, dass darauf keine personenbezogenen Daten mehr gespeichert sind.

TEIL D: Verarbeitung von papiergebundenen Akten

§ 29 Aufbewahrung von Akten

Akten und Schriftgut mit personenbezogenen oder sonstigen vertraulichen Daten sind so aufzubewahren, dass Unbefugte keinen Zugriff erhalten. Sie sind nach Dienstschluss verschlossen aufzubewahren. Wenn der zur Aufbewahrung der Akten oder des Schriftgutes verwendete Raum verlassen wird, ist er abzuschließen.

Es sind Maßnahmen zu treffen, die verhindern, dass Akten bei der Verarbeitung von Unbefugten eingesehen oder entwendet werden können.

Falls im Rahmen der Aufgabenwahrnehmung personenbezogene Daten in Akten außerhalb der Organisation bearbeitet werden müssen (z.B. im Außendienst oder bei Hausbesuchen), sind diese gegen unbefugte Zugriffe zu schützen. Sie sind nach Dienstschluss wieder in die Dienststelle zurückzubringen. Sofern dies nicht möglich ist, sind die Unterlagen bis zur Rückkehr in die Dienststelle an geeigneter Stelle verschlossen aufzubewahren.

§ 30 Versenden von Akten

Akten werden ausschließlich auf der Grundlage einer schriftlichen Anforderung (intern auch per E-Mail) übersandt. Die Versendung bedarf der vorherigen Genehmigung der Leitung der fachlich zuständigen Organisationseinheit, welche weitere Anweisungen für die Versendung erteilt.

Akten mit personenbezogenen Daten, die einem besonderen Amtsgeheimnis unterliegen (z.B. Personaldaten), dürfen auf dem internen Postweg oder an andere öffentliche Stellen (z.B. Gerichte) nur im verschlossenen Umschlag o.ä. versandt werden.

§ 31 Archivierung von Akten

Akten sind nach den spezialgesetzlichen Bestimmungen und den Vorgaben der KGSt behördenintern zu archivieren.

Behördenintern archivierten Akten sind spätestens nach Ablauf von 30 Jahren nach ihrer Entstehung dem Stadtarchiv anzubieten, wenn keine andere Frist durch eine vorrangige spezialgesetzliche Regelung bestimmt ist. Lehnt das Stadtarchiv eine Übernahme ab, sind die Akten datenschutzgerecht zu vernichten (§ 6 LDSG).

§ 32 Vernichtung von Akten

Die zur Vernichtung vorgesehenen Akten sowie nicht mehr benötigtes Schriftgut sind zeitnah zu vernichten. Soweit Schriftgut bis zur Vernichtung gesammelt wird, ist sicherzustellen, dass Unbefugte keine Kenntnis nehmen können. Hinsichtlich der Vernichtung sind die Anforderungen der aktuell gültigen DIN-Norm zu beachten.

Die/er behördliche Datenschutzbeauftragte ist zu informieren, falls große Mengen an Akten zu vernichten sind, die nicht mehr mit den bereitgestellten Aktenvernichtern zu bewerkstelligen sind.

TEIL E: Schlussbestimmungen

1. Beteiligung

Der Personalrat, die Gleichstellungsstelle der Stadt Speyer und die EDV-Abteilung waren an der Erstellung dieser Dienstanweisung beteiligt.

2. Schlussbestimmungen

Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft. Gleichzeitig tritt die Dienstanweisung für den Datenschutz bei der Stadtverwaltung Speyer vom 04.10.1994 außer Kraft.

Stadtverwaltung Speyer, den 9.5.2019

Stefanie Seiler
Oberbürgermeisterin

Anlagen

Anlage 1 (zu § 6)

Verpflichtung von Beschäftigten/Beamten zur Verschwiegenheit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)

Sehr geehrte/r Frau/Herr

da Sie ihm Rahmen Ihrer Tätigkeit mit personenbezogenen Daten in Kontakt kommen, verpflichte ich Sie hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit. Alle aus der Tätigkeit bekannt gewordenen oder anvertrauten personenbezogenen Daten sowie Angelegenheiten, die die Stadtverwaltung Speyer betreffen, sind streng vertraulich zu behandeln und dürfen nicht an Dritte weitergeben oder anderweitig verwertet oder verwendet werden**.** Ihre Verpflichtung besteht umfassend. Es ist Ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten.

Unter einer Verarbeitung versteht die DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittelung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Personenbezogene Daten im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierten oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn eine gesetzliche Regelung die Verarbeitung erlaubt, eine Verarbeitung dieser Daten vorgeschrieben ist oder eine Einwilligung vorliegt. Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

<u>Personenbezogene Daten müssen:</u>

a.) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

b.) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“)

c.) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (“Datenminimierung“)

d.) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)

e.) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“)

f.) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (“Integrität und Vertraulichkeit“)

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen / dienstrechtlichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeitsvertrag bzw. Dienstverhältnis oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Diese Verpflichtung besteht ohne zeitliche Begrenzung und gilt auch nach Beendigung der Tätigkeit weiter.

Ich bestätige durch meine Unterschrift die Verpflichtung sowie den Erhalt eines Exemplars der Verpflichtung.

Speyer, den

Ort, Datum	Unterschrift des/der Verpflichteten	Unterschrift des/der Verantwortlichen

Stadtverwaltung Speyer - behördlicher Datenschutz

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel

Name, Vorname

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Verarbeitungstätigkeit: Benennung: _____	**lfd. Nr.:** _____
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8*

…… …… .....
Verantwortlicher Datum Unterschrift

Anlage 3 (zu § 15)

Muster/Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO[1]

Hinweis:
Diese Formulierungshilfe ist nicht abschließend und bezieht sich in erster Linie auf die Fallgestaltung einer Auslagerung von klassischen IT-Dienstleistungen z. B. für die Lohnabrechnung oder Finanzbuchhaltung.
Je nach konkretem Anwendungsfall müssen gegebenenfalls weitere Inhalte hinzukommen, können solche weggelassen oder müssen modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden (z. B. bei Berufsgeheimnisträgern, bei Dienstleistungen zur Wartung, Datenlöschung oder -konvertierung, bei der externen Datenarchivierung).

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):

---

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag beginnt am ..... und endet am .....

---

[1] Diese Formulierungshilfe stellt keine Standardvertragsklauseln im Sinne von Art. 28 Abs. 8 DS-GVO dar.

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist .....

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

---

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 2 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privat- wohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

---

(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Sofern einschlägig:
Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

(Hinweis: Hier sind verschiedene Regelungsalternativen möglich. Die Parteien können ein absolutes Unterauftragsverbot vereinbaren, es kann aber auch ein Verbot mit Genehmigungsvorbehalt im Einzelfall geregelt werden. Auf letztere Möglichkeit bezieht sich der unten stehende Formulierungsvorschlag.)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage ..... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der

Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

(Hier haben die Vertragsparteien einen Gestaltungsspielraum: Entweder werden dem Auftragnehmer allgemein Befugnisse eingeräumt, Subunternehmer zu beauftragen oder dies wird von einer Einzelgenehmigung abhängig gemacht. Einigt man sich auf eine allgemeine Befugnis des Auftragnehmers zur Beauftragung von Subunternehmern, ist jede Subbeauftragung vorher durch den Auftragnehmer dem Auftraggeber anzuzeigen. Der Auftraggeber hat dann von Gesetzeswegen ein Recht auf Einspruch gegen diese Änderung (Art. 28 Abs. 2). Das Recht des Auftraggebers zum Einspruch ist im Vertrag ausdrücklich zu erwähnen. Da das Gesetz die Folgen dieses Einspruchs nicht regelt, wird empfohlen, hierzu vertragliche Regelungen zu finden. Wird keine Regelung getroffen, ist die Bestellung des Unterauftragnehmers, gegen den Einspruch erhoben wurde, nicht möglich.)

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitung derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

Das im Anhang …….. beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das im Anhang ……. beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:

> Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden am …… durch folgende unabhängige externe Stellen auditiert / zertifiziert gemäß den Regelungen nach Art. 42:
>
> ---
>
> Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

Oder:

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers icht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

dem Auftraggeber auszuhändigen.

oder

wie folgt datenschutzgerecht zu löschen bzw. zu vernichten / vernichten zu lassen:

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

---

11. Haftung

Auf Art. 82 DS-GVO wird verwiesen.
Im Übrigen wird folgendes vereinbart:

---

12. Vertragsstrafe

Bei Verstoß des Auftragnehmers gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro vereinbart.

13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Weitere Beispiele für mögliche Regelungen:

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Datum:

Unterschriften

Auftraggeber Auftragnehmer