Stadtwerke Schramberg GmbH & Co. KG • Postfach 581 • 78707 Schramberg

Muster GmbH
Muster Straße 0
00000 Musterstadt

Peter Kälble

Telefon: 07422-9534100
Telefax: 07422-9534101

Peter.kaelble
@stadtwerke-schramberg.de
www.stadtwerke-schramberg.de

23.10.2024

Auftragsdatenverarbeitungsvertrag gemäß Art. 28 DSGVO

Sehr geehrte Damen und Herren,

wir möchten für Sie und uns sicherstellen, dass unsere Leistungen im Rahmen unserer Zusammenarbeit die neuen datenschutzgrundrechtlichen Anforderungen erfüllen. Es kann im Rahmen unserer Kooperation vorkommen, dass Sie personenbezogenen Daten von der Stadtwerke Schramberg GmbH & Co. KG verarbeiten müssen.

Um Ihnen und uns hierfür die erforderliche Sicherheit zu geben, haben wir in Ergänzung zu unserem Vertrag eine Vereinbarung zur Auftragsdatenverarbeitung nach Artikel 28 DSGVO vorbereitet.

Wir bitten Sie, die beigefügte Vereinbarung in den „rot unterlegten Felder“ auszufüllen. Als Unterstützung erhalten Sie die folgende Tabelle.

→Bitte **ergänzen** Sie folgende Abschnitte in der beigefügten Vereinbarung:

Abschnitt	**Absatz**	**Erläuterungen**
1. Gegenstand und Dauer des Auftrags	(1)	Zeitpunkt des Vertragsabschlusses
2. Konkretisierung des Auftragsinhaltes	(1) - (3)	(1) Für welche Aufgaben werden pD[1] verarbeitet? (2) Welche Datenkategorien sind betroffen? (3) Von wem werden die Daten verarbeitet?
5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers	b)	Kontaktdaten des Datenschutzbeauftragten
6. Unterauftrags-verhältnisse	(2) a)	Auflistung der Unterauftragnehmer (Dienstleister, Subunternehmer etc.)
7. Kontrollrechte des Auftraggebers	(3)	Nachweis für die Umsetzung der TOM´s[2]

[1] personenbezogenen Daten
[2] Technische und Organisatorische Maßnahmen

Unterschrift des Auftragnehmers		
Anlage 1	6. Abweichungen des Auftragsnehmers	Abgleich von Soll- und IST-Situation bzgl. der TOM´s

Mit freundlichen Grüßen
Ihre Stadtwerke Schramberg GmbH & Co. KG

Peter Kälble

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO
(Bitte zutreffendes ankreuzen und fehlende vorhabenspezifische Angaben ergänzen)

Vereinbarung
zwischen der

Stadtwerke Schramberg GmbH & Co. KG, Gustav-Maier-Straße 11, 78713 Schramberg

- Verantwortlicher - nachstehend Auftraggeber genannt -
und dem/der

Muster GmbH, Musterstraße, 00000 Musterstadt

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags
(1) Der Gegenstand der Auftragsverarbeitung ergibt sich aus dem Vertrag und der Leistungsvereinbarung vom **14.09.2021.** Die bisher getroffenen Regelungen unter diesem Vertrag zu den Datenkategorien sowie dem Zweck der Verarbeitung gelten fort.

(2) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

2. Konkretisierung des Auftragsinhalts
(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.

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

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 und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau: hoch wird hergestellt durch verbindliche interne Datenschutzvorschriften.

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: **9. In Verbindung mit Anlage 5 Datenschutzerklärung**

oder

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien(Aufzählung/ Beschreibung der Datenkategorien):

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Sonstige:

(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
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Sonstige:.....

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

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

4. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, 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 er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

b) Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt

Name:_____

Organisationseinheit: _____

Adresse:_____

E-Mail: _____

Telefon:_____

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
d) 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 1].
e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
f) 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.
g) 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.
h) 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.
i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

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

(2)Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/ Land	Leistung

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(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 vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

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

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

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

- ☐ 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)

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

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

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. Weisungsbefugnis des Auftraggebers
(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

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

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

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

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift des Auftraggebers	Unterschrift des Auftragnehmers

Anlage 1

Technisch-organisatorische Maßnahmen zum Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Die folgende Anlage beschreibt technisch-organisatorische Maßnahmen, die für Verarbeitung von personenbezogenen Daten im Auftrag der Stadtwerke Schramberg GmbH & Co. KG einzuhalten sind[3].

Inhalt

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

1.1 Zutrittskontrolle
1.2 Zugangskontrolle
1.3 Zugriffskontrolle
1.4 Trennungskontrolle
1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
1.6 Weitergabekontrolle

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

2.1 Eingabekontrolle

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

3.1 Verfügbarkeitskontrolle
3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management
4.2 Incident Response Management
4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
4.4 Auftragskontrolle

5 Sonderregelung für Daten nach Art. 9 DSGVO

6 Abweichungen des Auftragnehmers

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

Grundsatz: Es wurden Maßnahmen ergriffen, die geeignet sind, Unbefugten den Zutritt, den Zugang und den Zugriff auf personenbezogene Daten zu verwehren.

[3] Sofern vom Auftragnehmer abweichende Regelungen zu einzelnen technisch-organisatorischen Maßnahmen in den jeweiligen Abschnitten angewendet werden, sind diese zu beschreiben und zu begründen (Abschnitt 6)

- ✓ Hierfür wurde ein Konzept zur Gebäude- und Raumsicherung umgesetzt sowie eine IT Sicherheits- und Datenschutzleitlinie erstellt, die technische und organisatorische Maßnahmen umfasst.

1.1 Zutrittskontrolle

1.1.1 Allgemeine Regel

- ✓ Es existiert ein technisch-organisatorisches Gesamtkonzept zur Zutrittskontrolle, das gestaffelte Sicherheitsregelungen für zentrale Datenverarbeitungsanlagen und Bereiche der Verarbeitung personenbezogener Daten (v.a. Kunden- und Personaldaten) umfasst.

1.1.2 Technische Maßnahmen

- ✓ Maßnahmen zum Gebäudeschutz (Außensicherung für nicht öffentliche Bereiche)
  - Es wird Sorge für einen gesteuerten Zutritt von Personen getragen.
    - Für Beschäftigte existiert eine Zutritts- und Anwesenheitsdokumentation mit elektronischem Schließsystem.
      Die erteilten Zutrittsberechtigungen werden regelmäßig überprüft und ggf. angepasst.
    - Eine Überwachung sämtlicher Haupt- und Nebeneingänge erfolgt entweder per Video oder Pförtner.
  - Die Verschließbarkeit sensibler Bürobereiche ist gewährleistet.
  - Es besteht die technische Möglichkeit sensible Dokumente verschlossen aufzubewahren.
- ✓ Zusätzliche Maßnahmen für Bereiche der Bearbeitung von Kunden- und Personaldaten
  - Büros oder Bereiche verfügen über Sicherheitsschlösser.
  - Sensoren für elementare Gefährdungen sind installiert.
  - Die Räumlichkeiten sind über eine Alarmanlage und Sicherheitsfenster geschützt.
- ✓ Zusätzliche Maßnahmen für zentrale Datenverarbeitungsanlagen
  - Der Bereich verfügt über Sicherheitsschlösser.
  - Der Zutritt wird mit einem elektronischen Schließsystem gesichert, Schließvorgänge werden protokolliert.
  - Eine Videoüberwachung von Eingang und Raum ist installiert.
  - Sensoren für elementare Gefährdungen sind installiert.
  - Die Räumlichkeiten sind über eine Alarmanlage und Sicherheitsfenster geschützt.

1.1.3 Organisatorische Maßnahmen

- ✓ Maßnahmen zum Gebäudeschutz (Außensicherung für nicht öffentliche Bereiche)
  - je nach Größe und baulichen Gegebenheiten gibt es eine angemessene Regelung zum offenen Tragen eines Mitarbeiterausweises oder zum gesicherten begleiteten Umgang mit Besuchern.
    - Vorherige Anmeldung/Identifikation von Besuchern an der Pforte
    - Protokollierung beim Zutritt und Verlassen mit einem offen zu tragenden Besucherausweis
    - Zutritt, Aufenthalt und Verlassen des Gebäudes erfolgen nur in Begleitung eines internen Mitarbeiters.
    - Die Nutzung von Foto-, Video-, Audio- und sonstigen Aufzeichnungsgeräten wie Mobiltelefone mit Kameras ist nur nach Genehmigung erlaubt.
  - Umgang mit Dienstleistern („Dauerbesucher“)
    - Es erfolgt eine sorgfältige Auswahl der Dienstleister.
    - Es erfolgt eine vollständige Protokollierung/Meldung der Namen der ausführenden Personen vor Antritt der Beschäftigung.
    - Beim erstmaligen Zutritt erfolgt eine Identifikation an der Pforte und die Ausgabe eines befristeten personalisierten Besucherausweises.
    - Dauerbesucherausweise sind offen zu tragen und nicht übertragbar.
- ✓ Zusätzliche Maßnahmen für Bereiche der Bearbeitung von Kunden- und Personaldaten
  - Bei Verlassen sind die entsprechenden Büros oder Bereiche zu verschließen.
  - Bildschirme sind so platziert, dass keine unbefugte Einsicht durch Besucher, Dienstleister oder nicht befugte Mitarbeiter möglich ist.
  - Sensible Dokumente sind beim Verlassen des Raumes wegzuschließen/vor Zugriff zu schützen (Clean Desk Police).
  - Der Bildschirm ist bei Verlassen zu sperren.

- ✓ Zusätzliche Maßnahmen für zentrale Datenverarbeitungsanlagen
  - Eine Verkeilung der Zugangstür ist untersagt.

1.2 Zugangskontrolle

1.2.1 Allgemeine Regel

- ✓ Es existiert eine IT Sicherheits- und Datenschutzrichtlinie mit technisch-organisatorischen Maßnahmen zur Verhinderung eines unbefugten Zugangs zu personenbezogenen Daten.

1.2.2 Technische Maßnahmen

- ✓ Passwortrichtlinie
  - Der Zugang zu Verarbeitungssystemen erfolgt ausschließlich mit persönlichem Login mit persönlichem Benutzernamen und Passwort.
  - Es ist eine technische Steuerung der vorgegebenen Passwortmindestanforderungen sowie zum regelmäßigen Wechsel des Passwortes implementiert.
- ✓ Abwehr von unbefugtem Zugang und Angriff auf die Infrastruktur
  - Die Infrastruktur ist durch Firewall, Anti-Viren-Software, ein Intrusion Detection/Prevention System bzw. Angriffserkennungssystem gesichert.
  - Remote Zugriffe erfolgen ausschließlich über VPN oder verschlüsselte Terminalserver-Verbindungen. Für den Zugang ist eine 2-Faktor-Authentifizierung implementiert.
  - Es finden regelmäßig Penetrationstests statt.
- ✓ Schutz mobiler Endgeräte
  - Die Daten mobiler Endgeräte sind verschlüsselt gespeichert und über eine Endpoint Protection Lösung gesichert.
  - Es erfolgt eine automatische Desktop-Sperre durch nicht veränderbare Konfiguration nach spätestens 15 Minuten.
  - Smartphones werden überein Mobile/Multi Device Management gesichert.
  - Mobile Datenträger sind nur zertifiziert und verschlüsselt zugelassen.
- ✓ E-Mail-Sicherheit
  - E-Mails werden bei Bedarf mit einer elektronischen Signatur versandt.
  - Eine technische Möglichkeit zur Verschlüsselung sensibler Mails ist vorhanden.

1.2.3 Organisatorische Maßnahmen

- ✓ Die Datenschutz- und IT Sicherheitsrichtlinie umfasst Regelungen zu folgenden Punkten:
  - Zentral dokumentierte Benutzerverwaltung und Benutzerrechtesteuerung (Verzeichnis der Verantwortlichen und Berechtigtengruppen).
    Die Benutzerverwaltung ermöglicht die Vergabe differenzierter Berechtigungen bezogen auf die Daten und auf die Bearbeitungsfunktionen.
  - Es existiert eine Richtlinie für die sichere Passwortvergabe für Systeme ohne technische Passwortsteuerung analog zur technischen Steuerung (s.o.).
  - Es wird eine Clean Desk Strategie verfolgt: Personenbezogene Unterlagen werden bei Verlassen des Arbeitsplatzes oder bei Nichtgebrauch verschlossen aufbewahrt.
  - Es existiert eine Regelung für das ordnungsgemäße Löschen/Vernichten und Entsorgen von Daten, Dokumenten und Datenträgern mit personenbezogenen Daten.
  - Eine Mobile Device Richtlinie enthält Anweisungen zu einem bewussten Umgang mit Daten und Datenträgern, die personenbezogene Daten enthalten können (u.a. Vermeidung der Einsichtnahme, Sperren des Bildschirms, WLAN Nutzung).

1.3 Zugriffskontrolle

1.3.1 Allgemeine Regel

- ✓ Es wurden Maßnahmen implementiert, die gewährleisten, dass die zur Benutzung eines Verarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen und personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1.3.2 Technische Maßnahmen

- ✓ Die Steuerung und Dokumentation von Zugriffsrechten erfolgt über ein zentrales Rechte- und Rollenmanagement.
- ✓ Es erfolgt eine Protokollierung von Zugriffen im Rahmen eines technisch und rechtlich angemessenen Umfangs.
- ✓ Es werden geeignete Einrichtungen zur sicheren Verwahrung und späteren Vernichtung von Daten und Datenträgern (Datentresor, externer Aktenvernichter nach DIN 32757, physische Löschung von Daten) bereitgestellt.
- ✓ Eine Überwachung des Netzwerkverkehrs ist implementiert mit folgenden Protokollierungen:
  - Daten über die Betriebsdauer von IT-Systemen (wann wurde welches IT-System ein- bzw. wieder ausgeschaltet?)
  - Zugriffe auf aktive Netzkomponenten (wer hat sich wann angemeldet?)
  - Sicherheitskritische Zugriffe auf Netzkomponenten und Netzmanagementkomponenten (erfolgreich/erfolglos)
  - Verteilung der Netzlast über die Betriebsdauer eines repräsentativen Zeitraumes

1.3.3 Organisatorische Maßnahmen

- ✓ Es ist eine Rollen- und Rechterichtlinie implementiert, die eine differenzierte Vergabe von Zugriffsrechten vorsieht und Regelungen für Autorisierung, Vergabe, Kontrolle, Aktualisierung und Entzug vorsieht.
  - Die Vergabe von Zugängen erfolgt nur insoweit, wie dies das Tätigkeitsprofil des Mitarbeiters erforderlich macht. Darüberhinausgehende Zugriffsberechtigungen und Zugänge werden nicht gewährt. Ändert sich das Tätigkeitsprofil, hat unverzüglich eine Anpassung der Berechtigungen zu erfolgen.
  - Die Entscheidung über die Angemessenheit von Berechtigungen und Zugängen sowie deren Genehmigung hat dabei stets durch den unmittelbaren Vorgesetzten des betroffenen Mitarbeiters zu erfolgen. Die Entscheidung ist dabei unter Betrachtung der Fähigkeiten des Mitarbeiters, der Kritikalität des Verarbeitungsprozesses für den Geschäftsbetrieb sowie der Klassifizierung der durch den Mitarbeiter zu verarbeitenden Informationen (bspw. kritische personenbezogener Daten) zu treffen.
  - Die verantwortlichen administrativen Stellen dürfen die Zuordnung von Zugängen und Zugriffen zum betroffenen Benutzeraccount des Mitarbeiters erst vornehmen, wenn die Genehmigung durch den Vorgesetzten des betroffenen Mitarbeiters in nachweisbarer Form vorliegt.
  - Die IT-Administration sowie die Vorgesetzten sind für eine regelmäßige Überprüfung und ggf. Anpassung der gewährten Zugriffe und Berechtigungen verantwortlich. Diese Überprüfung muss dokumentiert werden.

1.4 Trennungskontrolle

1.4.1 Allgemeine Regel

- ✓ Es werden abhängig von der Schutzbedarfsstufe Maßnahmen implementiert, die es uns ermöglichen, Daten, die zu unterschiedlichen Zwecken erhoben oder uns übergeben wurden, differenziert zu behandeln und zu verarbeiten.

1.4.2 Technische Maßnahmen

- ✓ Es erfolgt eine Trennung von Entwicklung-, Test- und Produktivumgebung.
- ✓ Für Prototyping und Test erfolgt bei Bedarf eine Bereitstellung einer separat gesicherten Umgebung („Sand-Box“).
- ✓ Eine Trennung der Zugriffe auf Daten und Systeme erfolgt je nach Anforderungen durch physische Trennung oder Virtualisierung des Netzwerkes.

1.4.3 Organisatorische Maßnahmen

- ✓ Die Trennungssteuerung erfolgt grundsätzlich über das Berechtigungskonzept.
- ✓ Die IT-Projektmanagement-Richtlinie beschreibt Verfahren zum sicheren Umgang mit Daten in Projekten.

- ✓ Im Projekt-Kick-off werden besondere Vorkehrungen zur Trennungskontrolle abgestimmt und entsprechende Anforderungen an den IT Service definiert. Deren Umsetzung wird periodisch kontrolliert.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

1.5.1 Allgemeine Regel

- ✓ Pseudonymisierung dient dem Schutz von Daten nach Art. 9 DSGVO (Verarbeitung besonderer Kategorien personenbezogener Daten) sowie der Definition der daraus abgeleiteten Maßnahmen nach Art. 25,1 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen). Unter Berücksichtigung des Stands der Technik werden im Rahmen der Auftragsprüfung (vgl. Abschnitt 4.4) die Implementierungskosten und Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen abgewogen und geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – definiert, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Daten-minimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

1.5.2 Technische Maßnahmen

- ✓ Ein technisches Verfahren zur Pseudonymisierung wird bedarfsorientiert nach Abschluss der Bewertung entsprechend Abschnitt 1.5.3 abgestimmt.

1.5.3 Organisatorische Maßnahmen

- ✓ Im Projekt-Kick-off wird bewertet, ob ein Verfahren zur Pseudonymisierung aufgrund der Sensitivität der Daten, der Weitergabe an Dritte oder wegen Art. 6,4 DSGVO (Verarbeitung von Daten, die ursprünglich zu anderen Zwecken erhoben wurden) notwendig sein sollte. Hierzu wird eine Bewertung technisch-organisatorischer Maßnahmen nach Art. 25,1 zur Minimierung von Daten durchgeführt und eine entsprechende Umsetzung konzipiert. Nach Abschnitt 4.4 unterliegt die Entscheidung über die Verarbeitung von Daten nach Art. 9 DSGVO einem Entscheidungsvorbehalt von Geschäftsführung und Datenschutzbeauftragtem.

1.6 Weitergabekontrolle

1.6.1 Allgemeine Regel

- ✓ Es wurden Maßnahmen implementiert, die gewährleisten, dass personenbezogene Daten bei der Übertragung oder während des Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es wird dabei auch überprüft, an welche Stellen eine Weitergabe vorgesehen ist und ob diese auch ordnungsgemäß durchgeführt wurde.

1.6.2 Technische Maßnahmen

- ✓ Für die Weitergabe von personenbezogenen Daten werden folgende technische Lösungen bereitgestellt:
  - Signaturverfahren für E-Mail und Dokumente
  - Verschlüsselung von E-Mails
  - Einsatz von VPN, Steuerung und Kontrolle der VPN-Zugriffe durch den Auftraggeber
  - Bereitstellung von verschlüsselten Verbindungen (https, S/Mime)
  - Bereitstellung sicherer Transportbehälter
  - Bereitstellung verschlüsselter Medien und Laufwerk

1.6.3 Organisatorische Maßnahmen

- ✓ Eine Weitergabe von personenbezogenen Daten erfolgt unter folgenden Bedingungen
  - Dokumentation von Beginn/Übergabe, Zeitdauer und Ende der Datenüberlassung (inkl. gesetzlicher oder vereinbarter Löschfristen)
  - Bewertung der Erforderlichkeit der Übergabe in einer pseudonymisierten Fassung (s.o.)
  - Eindeutige Definition und Identifikation autorisierter Personen für Transport und Übergabe

- Sorgfältige Bewertung und Auswahl der Übertragungs- und Transportwege/-mittel

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

Grundsatz: Es wurden Verfahren implementiert, die gewährleisten, dass personenbezogene Daten vor unrechtmäßiger Verarbeitung durch Unbefugte und gegen unbeabsichtigte Schädigung und Verlust geschützt sind.

2.1 Eingabekontrolle

2.1.1 Allgemeine Regelungen

- ✓ Es wurden Maßnahmen implementiert, die angemessen gewährleisten, dass - datenschutzkonform - auch nachträglich überprüft werden kann, ob und von wem personenbezogene Daten verarbeitet wurden (Eingabe, Veränderung, Löschung).

2.1.2 Technische Maßnahmen

- ✓ Zur Speicherung und Archivierung von Dokumenten werden Systeme eingesetzt, die die personalisierte und revisionssichere Speicherung sowie Versionskontrolle von Dokumenten ermöglichen.
- ✓ Aktivitäten in den eingesetzten Systemen werden protokolliert (Log-Dateien). Hierzu sind folgende Regelungen vereinbart:
  - Verantwortliche für die Durchführung der technischen Protokollierung sind benannt.
  - Die technische Protokollierung umfasst neben den Benutzern auch eine Protokollierung von Administratorenaktivitäten.
  - Es ist definiert, in welchen Abständen und zu welchen Anlässen Einsicht in diese Protokolle genommen werden darf.
  - Die Aufbewahrungs- und Löschfristen dieser Protokolle sind definiert.

2.1.3 Organisatorische Maßnahmen

- ✓ Die eingesetzten technischen Verfahren sind hinreichend dokumentiert, Nutzer und Administratoren werden vor Inbetriebnahme von Systemen sorgfältig geschult, so dass eine ordnungsgemäße Nutzung der Systeme gewährleistet ist.
- ✓ Die Zuordnung von Eingabebefugnissen erfolgt auf der Basis von Zweckbindung und Minimierung/Sparsamkeit bei der Zuteilung von Rechten und Rollen.

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

Grundsatz: Es wurden Maßnahmen implementiert, die die Fähigkeit der Systeme sichern, trotz massiver externer oder interner Störungen wieder in den Ausgangszustand zurückzukehren.

3.1 Verfügbarkeitskontrolle

3.1.1 Allgemeine Regel

- ✓ Es wurden Maßnahmen implementiert, die gewährleisten, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind.

3.1.2 Technische Maßnahmen

- ✓ Die zentralen Datenverarbeitungsanlagen sind mit USV/NSV und Überspannungsschutz ausgestattet.
- ✓ Die zentralen Datenverarbeitungsanlagen sind mit Klimatisierung und Elementarschadensschutz ausgestattet.
- ✓ Es werden regelmäßig Datensicherungen durchgeführt. Die Sicherungen werden an einem sicheren und geschützten Aufbewahrungsort in hinreichender Entfernung von den Verarbeitungssystemen aufbewahrt.
- ✓ Das Netzwerk ist in seinen wichtigen Komponenten geschützt und möglichst redundant ausgelegt.
- ✓ Die Räumlichkeiten verfügen über eine Brandmelde- und/oder Löschanlage (mind. Handfeuerlöscher).
- ✓ Eine robuste Verfügbarkeit im Regelbetrieb erfolgt durch eine vollständige Virtualisierung der Serverlandschaft sowie durch eine sichere SAN-Infrastruktur.

3.1.3 Organisatorische Maßnahmen
- ✓ Die Vorgehensweisen bei Backup und Recovery sind in einem Notfallkonzept beschrieben. Es werden regelmäßige Tests zur Wiederherstellung der Systeme durchgeführt.
- ✓ Ein hinreichendes Kapazitätsmanagement für die Systeme und Verfahren wurde etabliert. Technische Versorgungseinrichtungen, wie z.B. Klimaanlagen, Stromversorgung, Brandschutz sind hinreichend dimensioniert und werden regelmäßig, in den entsprechenden Intervallen, gewartet. Dies ist durch Wartungsprotokolle nachweisbar.
- ✓ Es wurden dokumentierte Prozesse für kontrollierte Änderungen in den Verarbeitungssystemen etabliert.
- ✓ Brandlasten (z.B. Papier, IT-Equipment, sonstige Vorräte) dürfen nicht in unmittelbarer Nähe oder innerhalb des Serverraums selbst gelagert werden. Die Lagerung von Altgeräten, Ersatzteilen, Elektroschrott und sonstigem Material im IT-Raum ist untersagt.

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

3.2.1 Allgemeine Regel
- ✓ Im Notfallkonzept wurden Verfahren zur raschen Wiederherstellung von Daten und Verarbeitungssystemen implementiert.

3.2.2 Technisch-organisatorische Maßnahmen
- ✓ Die rasche Wiederherstellung bei Teilausfällen erfolgt auf Basis virtualisierter Server- und Speichersysteme sowie durch den Einsatz entsprechend leistungsfähiger Backup-Restore-Mechanismen.
- ✓ Die Wiederherstellung bei einem funktionalen Vollausfall ohne physische Zerstörungen erfolgt durch das Einspielen der hinterlegten Sicherungskopien.
- ✓ Die Wiederherstellung bei einem Vollausfall mit physischer Zerstörung erfolgt anhand eines strukturierten Prozesses zur vollständigen Rekonstruktion des Rechenzentrums.
- ✓ Durch Bereitschaftsstrukturen ist sichergestellt, dass in Notfällen umgehend reagiert werden kann.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DSGVO)

Grundsatz: Das Datenschutz-Management-System ist Teil eines integrierten Management-Systems (IMS) und folgt dessen Governance-Prinzipien.

4.1 Datenschutz-Management

4.1.1 Allgemeine Regel
- ✓ Es wurden Verfahren implementiert, die ein ordnungsgemäßes Datenschutzmanagement ermöglichen und kontinuierlich für eine Aktualisierung und Verbesserung sorgen.

4.1.2 Technische Maßnahmen
- ✓ Software-gestützte Dokumentation der Verfahren
- ✓ Software-gestützte Dokumentation der Datenschutzfolgenabschätzung
- ✓ Dokumentation der technisch-organisatorischen Maßnahmen (TOMS) im Intranet

4.1.3 Organisatorische Maßnahmen
- ✓ Der Datenschutzbeauftragte ist bestellt.
- ✓ Eine regelmäßige Unterrichtung der Führungsebene ist sichergestellt.
- ✓ Die Mitarbeiter sind unterrichtet und verpflichtet.
- ✓ Jährlich findet eine Sensibilisierung der Mitarbeiter statt.
- ✓ Die Abstimmung mit dem Informationssicherheitsbeauftragten und dem ISMS-Verantwortlichen ist etabliert.
- ✓ Eine Datenschutzfolgenabschätzung wird bedarfsorientiert durchgeführt und regelmäßig evaluiert.
- ✓ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach.
- ✓ Auskunftsanfragen von Betroffenen werden ordnungsgemäß und strukturiert bearbeitet und beantwortet.
- ✓ Es ist ein jährlicher Prozess etabliert, der die Datenschutzdokumentation sowie die Maßnahmen zum Datenschutz überprüft, bewertet und bei identifiziertem Bedarf fortschreibt

4.2 Incident Response Management

4.2.1 Allgemeine Regel

- ✓ Es wurden Verfahren implementiert, die bei Bedrohungen oder Verletzungen in der Lage sind, mögliche Schäden abzuwehren und zu managen.

4.2.2 Technische Maßnahmen

- ✓ s. 1.1.2 technische Maßnahmen zur Zugriffskontrolle

4.2.3 Organisatorische Maßnahmen

- ✓ Ein Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und deren Meldung an die Aufsichtsbehörden ist etabliert.
- ✓ Eine dokumentierte Vorgehensweise zum Umgang mit Vorfällen ist vorhanden.
- ✓ Bei Vorfällen werden DSB und ISB eingebunden.
- ✓ Die Dokumentation und Informationsweitergabe von Sicherheitsvorfällen erfolgt in nicht vom Vorfall kompromittierten Systemen.
- ✓ Vorgehensweisen und Verantwortlichkeiten zur Nachbearbeitung, Forensik, Auswertung und Empfehlungen sind definiert.
- ✓ Für kritische Aufgaben des Incident Management wurde für Redundanz gesorgt.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

4.3.1 Allgemeine Regel

- ✓ Es wurden Maßnahmen implementiert, die aufgrund von Voreinstellungen der Systeme das Risiko von Datenschutzbedrohungen oder gar verletzungen reduzieren oder verhindern (Privacy by Design, Privacy by Default).

4.3.2 Technisch-organisatorische Maßnahmen

- ✓ Es wurde eine Daten- und Speicherminimierungsstrategie zur Überprüfung der Daten als auch der Verarbeitungsprozesse nach gesetzlicher Zulässigkeit und Erforderlichkeit etabliert.
- ✓ Bei neu aufgenommenen Daten erfolgt eine Dokumentation hinsichtlich der gesetzlichen Verarbeitungsgrundlagen.
- ✓ Es wurde für Einwilligungen ein Verfahren zur Sicherstellung des Widerrufsrechtes und für Löschanforderungen von Betroffenen etabliert.
- ✓ In den Verfahren wird der Stand der Technik im User Interface Design und der Nutzerführung eingesetzt, um mögliche Benutzerfehler zu vermeiden.
- ✓ Soweit technisch verfügbar, wirtschaftlich vertretbar und gesetzlich zulässig werden technische Verfahren zur Plausibilisierung und Konsistenzsicherung von personenbezogenen Daten einsetzen

4.4 Auftragskontrolle

4.4.1 Allgemeine Regel

- ✓ Es wurden Maßnahmen implementiert, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich im Rahmen und entsprechend den Weisungen des Auftraggebers verarbeitet werden. Diese Maßnahmen gelten sowohl für die Rolle als Auftraggeber als auch als Auftragnehmer.

4.4.2 Technisch-organisatorische Maßnahmen

- ✓ Sofern beabsichtigt ist, personenbezogene Daten zu verarbeiten, wird ein Auftragsverarbeitungsvertrag abgeschlossen. Gegenstand dieses Vertrages ist es, neben den grundsätzlichen rechtlichen Festlegungen eine Übereinkunft über folgende Sachverhalte zu treffen und diese zu dokumentieren:
  - Grundlegende Feststellung, ob es sich um einen Auftragsdatenverarbeitungsvertrag nach Art. 28 DSGVO handelt oder um Funktionsübertragung technischer Dienstleistungen. Eine Auftragsdatenverarbeitung liegt vor, wenn der Dienstleister die an ihn delegierte Datenverarbeitung, als „verlängerter Arm“ des Auftraggebers, streng weisungsgebunden und ohne eigene Entscheidungsbefugnis durchzuführen hat, insbesondere dann, wenn das Kerngeschäft die Verarbeitung personenbezogener Daten ist (z.B. Prüfung der Angemessenheit von CVs, Konfiguration eines CRM-Systems).

Eine Funktionsübertragung liegt vor, wenn dem Dienstleister bei der Datenverarbeitung eine gewisse Eigenverantwortlichkeit und Entscheidungsbefugnis zukommt, die seine Tätigkeit über die reine Hilfsfunktion hinaushebt, vor allem dann, wenn die Verarbeitung personenbezogener Daten nur eine Randbedingung oder Voraussetzung der Erfüllung eines Vertrages ist und nicht dessen Hauptbestandteil (z.B. Verwaltung von Kontaktdaten für das Projektmanagement).

- Prüfung und Sicherstellung eines verabredeten Schutzniveaus, von dem Tiefe und Reichweite der daraus folgenden TOMs abhängt
- Verabredung der TOMs Maßnahmen zur Weitergabe von Daten bzw. zu deren Zugang, Zugriff und Übermittlung
- Verabredung der datenschutzkonformen Abnahme bei Beendigung des Vertrages (Übergabe, Löschung von personenbezogenen Daten)
- Bei Erweiterungen oder Einschränkungen des Leistungsumfangs Anfordern von schriftlichen Weisungen
- Grundsätzliches Einverständnis zur Wahrnehmung von Kontrollmechanismen und Pflichten

5 Sonderregelung für Daten nach Art. 9 DSGVO

Verarbeitungsaufträge zur Verarbeitung von Daten nach Art. 9 DSGVO (zum Beispiel Gesundheitsdaten, genetische und biometrische Daten, sexuelle Orientierung, politische, religiöse, gewerkschaftliche, ethnische Herkunft usw. bedürfen der vorherigen Freigabe durch die Geschäftsführung und den Datenschutzbeauftragten). Eine Verarbeitung erfolgt vorbehaltlich einer Datenschutzfolgenabschätzung und der Umsetzung daraus resultierender Maßnahme.

6. Abweichungen des Auftragnehmers

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 Abweichungen bei Vertragsbeginn sind hier zu dokumentieren

Nr.	Titel	Abweichung	Begründung
1	***Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)***		
1.1	*Zutrittskontrolle*		
1.2	*Zugangskontrolle*		
1.3	*Zugriffskontrolle*		
1.4	*Trennungskontrolle*		
1.5	*Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)*		
1.6	*Weitergabekontrolle*		
2	**Integrität (Art. 32 Abs. 1 lit. b DSGVO)**		
2.1	Eingabekontrolle		
3	**Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**		
3.1	*Verfügbarkeitskontrolle*		
3.2	*Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)*		
4	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DSGVO)**		
4.1	*Datenschutz-Management*		
4.2	*Incident Response Management*		
4.3	*Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)*		
4.4	*Auftragskontrolle*		
5	**Sonderregelung für Daten nach Art. 9 DSGVO**		