Anlage 1: Allgemeine Vorschriften Datenschutz und Informationssicherheit (AVDI) (Stand: 17.01.2023)

1 Präambel

(1) Diese AVDI basieren auf der EU-DSGVO (EU-Datenschutz-Grundverordnung) und insbesondere Festlegungen nach Art. 28 EU-DSGVO zur Auftragsverarbeitung, sowie den Erweiterungen und Konkretisierungen der EU-DSGVO im BDSG-neu (Bundesdatenschutzgesetz). Diese Festlegungen stellen an den Auftraggeber wie den Auftragnehmer zusätzliche Anforderungen. Beide Parteien haben bei Missachtung mit empfindlichen Bußgeldern bis hin zum Verbot der Datenverarbeitung zu rechnen.
(2) Obwohl Wartung, Pflege, Softwareentwicklung und/oder Service prinzipiell vom Auftraggeber so gestaltet werden können, dass auf IT-Ebene ein Zugriff auf personenbezogene Daten durch den Auftragnehmer ausgeschlossen werden könnte, ist dieser Ausschluss praktisch oft nicht umsetzbar. Entsprechend unterwirft sich der Auftragsnehmer den strengen Regeln der Auftragsverarbeitung und unterstützt den Auftraggeber bei der Einhaltung und Umsetzung dieser gesetzlichen Anforderungen nach Art. 28 EU-DSGVO.

2 Vertragliche Beziehungen

(1) Zwischen Auftraggeber und Auftragnehmer werden als Ergänzung zu allen zwischen den Parteien bestehenden Vereinbarungen, anlässlich derer der Auftragnehmer oder durch ihn beauftragte Dritte in Kontakt mit personenbezogenen Daten im Sinne der EU-DSGVO kommen, die nachfolgenden Regelungen getroffen.
(2) Die Datenverarbeitung erfolgt durch den Auftragnehmer als weisungsgebundene Tätigkeit nach Maßgabe der nachstehenden Vereinbarungen im Auftrag des Auftraggebers im Sinne von Art. 28 Abs. 3a) EU-DSGVO. Gegenüber den betroffenen Personen und Dritten trägt allein der Auftraggeber die Verantwortung für die Zulässigkeit der in seinem Auftrag durchgeführten Verarbeitungen personenbezogener Daten, soweit dies nicht anders spezifiziert wurde oder gesetzlich vorgesehen ist.
(3) Die Datenverarbeitung im Auftrag als gemeinsame, gleichberechtigte Verantwortungsaufgabe von Auftraggeber und Auftragnehmer nach Artikel 26 EU-DSGVO findet nicht statt.

3 Definitionen

(1) Der Auftraggeber ist **Verantwortlicher** gemäß Art. 4 Nr. 7 EU-DSGVO. Der Auftragnehmer ist **Auftragsverarbeiter** gemäß Art. 4 Nr. 8 EU-DSGVO. **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
(2) **Datenverarbeitung im Auftrag** ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.
(3) **Verarbeitung** meint die Verwendung personenbezogener Daten. Diese umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung / Einschränkung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

4 Umfang, Art, Zweck der Erhebung

(1) Der Umfang, Art und Zweck der Erhebung sind in einer oder mehreren Meldungen zum Verzeichnis von Verarbeitungstätigkeiten des Auftraggebers nach Art. 30 EU-DSGVO niedergelegt, bei den die Dienstleistungen des Auftragnehmers eingesetzt werden bzw. im Nachweis der Rechenschaftspflicht nach Art. 5 Abs. 2 EU-DSGVO für die Grundsätze für die Verarbeitung personenbezogener Daten i.S.v. Art. 5 Abs. 1 EU-DSGVO. Der Auftragnehmer hat keinen Einfluss auf die Dokumentation von Verarbeitungstätigkeiten und die Nachweise der Rechenschaftspflicht beim Auftraggeber. Typische Zwecke können sein: Vertragsanbahnung, Data Warehousing, Vertragsabwicklung, geschäftsmäßige Übermittlung u.v.m.
(2) Anlässlich der Durchführung der betroffenen Verträge ist es nicht ausgeschlossen, dass der Auftragnehmer zufällig Kenntnis von personenbezogenen Daten erhält.

5 Arten der Daten und Kreis der Betroffenen

(1) Die durch den Auftraggeber erzeugten Daten können sowohl „einfache" personenbezogene Daten darstellen als auch besondere personenbezogene Daten (sensible Daten) im Sinne von Art. 9 Abs. 1 EU-DSGVO sein.
(2) Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die der Auftraggeber auf Systemen des Auftragnehmers verarbeitet, z.B. Stammdaten, Leistungsdaten Lohndaten, Vertragsdaten, Bankdaten, Finanzdaten Umsatzdaten, Bestelldaten, Logistikdaten, Qualifikationsdaten. Der Auftragnehmer hat keinen Einfluss auf die Art der personenbezogenen Daten, die der Auftraggeber verarbeitet. Näheres hierzu findet sich im Verarbeitungsverzeichnis des Auftraggebers (siehe 4.1).
(3) Die Kategorien betroffener Personen sind abhängig von der Art des Einsatzes der Systeme beim Auftraggeber. Der Auftragnehmer hat keinen Einfluss auf diese Kategorien. Diese können z.B. sein: Auszubildende, Beschäftigte und Interessenten sowie Geschäftspartner des Auftraggebers, Beschäftigte, Familienangehörige und Geschäftspartner der Interessenten des Auftraggebers, andere Personen, ggf. auch als Verbraucher, sofern der Auftraggeber Daten über sie verarbeitet auf den System den Auftragnehmers. Näheres hierzu findet sich im Verarbeitungsverzeichnis des Auftraggebers (siehe 4.1).
(4) Der Auftraggeber sichert dem Auftragnehmer zu, dass die personenbezogenen Daten rechtmäßig erhoben wurden. Kommt es zu einer Schädigung beim Auftragnehmer aufgrund einer nicht rechtskonformen Erhebung, dann übernimmt der Auftraggeber die durch die Schädigung entstandenen die Kosten.

6 Berichtigung, Sperrung und Löschung von Daten, Betroffenenrechte

(1) Der Auftragnehmer wird ohne Weisung des Auftraggebers keine Berichtigung, Sperrung oder Löschung von Daten vornehmen. Die Parteien stellen klar, dass eine solche Nutzung nicht Gegenstand der Verträge i. S. v Ziffer 2 ist.
(2) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anfragen von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten.
Wenn eine betroffene Person etwaiger Ansprüche nach Art. 82 EU-DSGVO gegenüber dem Auftraggeber erhebt und wenn diese Ansprüche auf Verarbeitungen beruhen, an denen der Auftragnehmer im Rahmen dieses Vertragsverhältnisses beteiligt ist, dann verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
(3) Eine durch den Auftragnehmer erforderliche Unterstützung erfolgt gegen Aufwand und wird dem Auftraggeber zu den jeweils aktuell gültigen Konditionen vom Auftragnehmer in Rechnung gestellt.

7 Weisungen des Auftraggebers

(1) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Der Auftraggeber ist berechtigt, vollumfänglich Weisungen zu erteilen. Mündliche Weisungen hat der Auftraggeber schriftlich zu bestätigen.

8 Erforderliche Verpflichtung

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers den Datenschutz gemäß EU-DSGVO / BDSG-neu sowie gem. § 3 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) sowie ggf. Sondergesetzen wie z.B. SGB V zu wahren. Er verpflichtet sich also, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Soweit der Auftraggeber Sondergesetzen des Datenschutzes unterliegt, die über EU-DSGVO, BDSG-neu, Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), ist der Auftraggeber

verpflichtet, den Auftragnehmer auf die Geltung dieser Gesetze ausdrücklich hinzuweisen. Der Auftragnehmer wird sodann unverzüglich seine daraus folgenden Verpflichtungen feststellen und einhalten. Er wird nur Mitarbeiter beschäftigen, deren Zuverlässigkeit und Vertrauenswürdigkeit er sich zuvor versichert hat. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die Einhaltung der datenschutzrechtlichen Vorschriften überwacht. **Der Auftragnehmer sichert zu, dass seine mit der Verarbeitung der Daten des Auftraggebers beschäftigten Mitarbeiter stets auf die Vertraulichkeit im Sinne der EU-DSGVO sowie gem. § 3 TTDSG schriftlich auf das Daten- und das Fernmeldegeheimnis verpflichtet sind.**
(2) Die Verarbeitung der Daten 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. EU-DSGVO erfüllt sind.
(3) Auskünfte über Daten und Gegebenheiten im Zusammenhang mit der Auftragsausführung des Auftragnehmers für den Auftraggeber darf der Auftragnehmer Dritten gegenüber nur nach vorheriger schriftlicher Zustimmung erteilen. In diesem Vertrag ausdrücklich geregelte oder gesetzlich vorgeschriebene Auskunftsrechte bzw. Auskunftspflichten bleiben hiervon unberührt. Auskünfte nach Datenschutzrecht erteilt allein der Auftraggeber als Verantwortlicher. An der Erstellung notwendiger Verarbeitungsbeschreibungen hat der Auftragnehmer auf Anforderung des Auftraggebers mitzuwirken. Er hat dem Auftraggeber insoweit die erforderlichen Angaben zuzuleiten. Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der in diesem Vertrag vereinbarten sowie der allgemeinen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO zu. Er wird also seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird TOMs zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen. Der Auftragnehmer dokumentiert von Ihm ergriffene Maßnahmen zur Einhaltung seiner Verpflichtungen aus den vorstehenden Ziffern schriftlich und nachvollziehbar.

9 Geschäftsgeheimnis

(1) Der Auftragnehmer verpflichtet sich, über nicht allgemein bekannte, geschäftlich relevante und bedeutsame Angelegenheiten des Auftraggebers (Geschäftsgeheimnisse) Verschwiegenheit zu wahren. Er wird auch seine Mitarbeiter zur Verschwiegenheit verpflichten, vgl. dazu auch 8(1). Dem Auftraggeber bleibt es unabhängig davon unbenommen, entsprechende Verschwiegenheitsverpflichtungen direkt mit den Mitarbeitern des Auftragnehmers zu vereinbaren.
(2) Soweit nicht näher im Hauptvertag beschrieben, gilt, dass sich die Parteien zu strikter Vertraulichkeit Dritten gegenüber verpflichten. Die Parteien sind insbesondere verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekannt werdenden Geschäfts- und Betriebsgeheimnisse, Herstellungsverfahren, Arbeitsmethoden und sonstigen geschäftlichen bzw. betrieblichen Tatsachen, Unterlagen und Informationen der anderen Partei sowie ihrer Kunden und Geschäftspartner streng vertraulich zu behandeln, in keiner Weise Dritten zugänglich zu machen oder sonst zu verwenden, vorbehaltlich anderer vertraglicher Absprachen. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig.

10 Technische und organisatorische Maßnahmen (TOM) und Nutzung von Zertifikaten (z.B. ISO 27001), Testaten und Selbstauskünften

(1) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft TOMs zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust, die den Forderungen des Art. 32 DSGVO entsprechen
(2) Insbesondere sichert der Auftragnehmer die Einhaltung der TOMs zu, die er in der Anlage 2 **Selbstauskunft TOMs** aufgeführt hat. Die TOMs unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insbesondere ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
Der Auftragnehmer aktualisiert die Liste der TOMs im Anlage 2 regelmäßig und lässt diese dem Auftraggeber zur Kontrolle zukommen.
(3) Verfügt der Auftragnehmer über ein datenschutzrelevantes Zertifikat, kann dieses unter folgenden Voraussetzungen zur Unterstützung der Vorabkontrollen und Überwachungen durch den Auftraggeber genutzt werden:

1. Das Zertifikat muss gültig sein.
2. Die Auftragsverarbeitung des Auftragsnehmers muss im Scope (Anwendungsbereich) der Zertifizierung liegen.
3. Das Statement of Applicability (SoA/ Anwendbarkeitserklärung) darf keine Ausschlüsse aufweisen hinsichtlich der in Art. 32 EU-DSGVO genannten TOMs.
4. Es werden lückenlos interne und externe Audits durchgeführt.
5. Der Auftraggeber bekommt auf Anforderung Einsicht in den letzten Audit-Report.

Ebenso können Datenschutz-Testate von sachverständigen Dritten sowie Selbstauskünfte des Auftragnehmers Verwendung finden.

Der Auftragnehmer verfügt über folgende Zertifizierungen und Testate:

- keines

die den oben genannten Anforderungen entsprechen.

11 Ansprechpartner

Die Parteien sind sich darüber einig, dass es notwendig ist, Regelungen zur Kommunikation zu treffen, um eine sichere, störungsfreie und datenschutzgerechte Auftragsausführung zu gewährleisten. Der Auftragnehmer hat den Auftraggeber vor wichtigen Eingriffen in das IT-System über beabsichtigte Änderungen und Eingriffe unverzüglich zu informieren und diese nur nach entsprechender Freigabe durch den Auftraggeber zu veranlassen bzw. durchzuführen. Die Parteien benennen wechselseitig Ansprechpartner und werden diesbezügliche Änderungen dem jeweils anderen Vertragspartner unverzüglich schriftlich mitteilen. Der Auftragnehmer darf Auskünfte ausschließlich gegenüber den vom Auftraggeber autorisierten Personen erteilen. Der Auftragnehmer verpflichtet sich durch TOMs sicherzustellen, dass nur die für die Auftragsbearbeitung erforderlichen Mitarbeiter Zugang zu den zu betreuenden IT-Systemen und Zugriff auf die zu verarbeitenden Daten des Auftraggebers erlangen können (need-to-know-Prinzip). Die Parteien benennen ihre jeweiligen Ansprechpartner in Anlage 3: Liste der Ansprechpartner.

12 Pflichten, Kontroll- und Betretungsrechte, Meldepflichten

(1) Der Auftragnehmer arbeitet datenschutzrechtlich ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Er verwendet etwaige zur Verarbeitung überlassene Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und sonstige Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Durchführung des Auftrages erforderlich sind, sowie Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen.
Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(2) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Meldung zum Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO notwendigen Angaben zur Verfügung. Ebenso unterstützen sich Auftragnehmer und Auftraggeber soweit vertretbar und geboten bei etwaigen Datenschutzfolgenabschätzung, die im Bereich dieser AVDI oder dem Hauptvertag liegen.
(3) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen (insbesondere bei Verdacht auf meldepflichtige Verletzungen des Schutzes personenbezogener Daten nach Art. 33 EU-DSGVO) oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 und Art. 34 EU-DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften, Testaten eines Sachverständigen, Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie Betreten und Besichtigung der Räumlichkeiten des Auftragnehmers, welche die Leistungserbringung für den Auftraggeber betreffen. Der Auftragnehmer verpflichtet sich insoweit dem Auftraggeber oder von diesem beauftragten Dritten (Prüfer, Auditoren) zu diesem Zwecke Zugang zu den Firmenräumen zu gewähren, sofern diese nicht in einem Wettbewerbsverhältnis mit dem Auftragnehmer stehen oder andere berechtigte Gründe seitens des Auftragnehmer dem entgegenstehen. Wenn diese Prüfungen erhebliche Mehrkosten beim Auftragnehmer verursachen, dann trägt diese Kosten der Auftraggeber.
(4) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten datenschutzrechtlich relevante Unterlagen und erstellten datenschutzrechtlich relevante Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Vertragsverhältnis im Sinne von Ziffer 2 stehen, dem Auftraggeber auszuhändigen. Die verwendeten Datenträger des Auftragnehmers sind danach soweit technisch möglich physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung beziehungsweise Übergabe. Überlassene Datenträger sowie sämtliche hiervon gefertigte Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe, Löschung oder Aufbewahrung der Daten, so trägt diese der Auftraggeber.

13 Subunternehmer/Unterauftragnehmer

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 4 zu diesem Vertrag angeben.
Der Auftragnehmer informiert den Auftraggeber schriftlich über beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter bzw. Subunternehmer. Hierdurch erhält der Auftraggeber die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben. Dieser Einspruch muss zwingend datenschutzrechtlich begründet sein. Dies können auch datenschutzrechtlich begründete Interessenskonflikte sein. Sonstige Interessenskonflikte sind fernab des Auftragsverarbeitungsvertrages im Hauptvertrag zu regeln.
Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist von 4 Wochen widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.
Für den Fall eines Einspruchs ist dem Auftraggeber bewusst, dass dies ein schwerer Eingriff in die allgemeinen Betriebsabläufe des Auftragnehmers bedeutet, der auch andere Auftraggeber des Auftragnehmers unmittelbar betrifft. Daher sichert der Auftraggeber zu, bei einem solchen Einspruch die Verhältnismäßigkeit zwischen seinem Schutzbedürfnis und der Schwere des Eingriffs für den Auftragnehmer zu berücksichtigen. Auftraggeber und Auftragnehmer werden sich daher auch im Falle des Einspruchs bemühen, eine einvernehmliche Lösung zu finden. Sollte keine einvernehmliche Lösung gefunden werden, dann haben beide Vertragsparteien ein außerordentliches Kündigungsrecht.
(2) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag an diese zu übertragen und zu prüfen, insbesondere dahingehend, dass TOMs nach Art. 32 EU-DSGVO umgesetzt sind. Erst danach ist eine Weiterleitung von Daten zulässig.
(3) Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Dem Auftraggeber werden Kontroll- und Überprüfungsrechte entsprechend Ziffer 10 eingeräumt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
(4) Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer von Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen u.a. Lohnbuchhaltungs- und Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern.

14 Informationspflichten, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als verantwortlicher Stelle im Sinne der EU-DSGVO liegen. Es gilt deutsches Recht.
(2) Die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ist ausgeschlossen.

15 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt.

1 Anlage 2: Selbstauskunft TOM (Stand: 17.01.2023)

Folgende technische und organisatorische Maßnahmen werden vom Auftragnehmer umgesetzt. Auf Grundlage von Art. 25 und insbesondere Art. 32 EU-DSGVO gibt der Auftragnehmer hier an, welche technischen und organisatorischen Maßnahmen er zur Gewährleistung des Datenschutzes und der Datensicherheit getroffen hat. Wenn anwendbar und vertretbar wird eine Maßnahme nach dem Stand der Technik durchgeführt, dies gilt insbesondre für Verschlüsselungsverfahren.

Die Folgende Auflistung gibt eine Übersicht der TOMs nach Maßnahmenbereichen an. Der Auftraggeber hat die Möglichkeit die umfassende und detaillierte Aufstellung aller datenschutz- und informationssicherheitsrelevanter TOMs aus den Maßnahmenbereichen anzufordern. Wenn diese Prüfungen erhebliche Mehrkosten beim Auftragnehmer verursachen, dann trägt diese Kosten der Auftraggeber.
In allen folgenden Maßnahmenbereichen wurden TOMs – soweit anwendbar - zur Gewährung eines angemessen Datenschutz- und Informationssicherheitsniveaus eingeführt.

2 Standorte der Datenverarbeitung

Die Firma Sigma-IT GmbH betreibt die benötigten IT-Systeme im Wortmann Rechenzentrum in Hüllhorst (TERRA CLOUD GmbH, Hankamp 2, 32609 Hüllhorst, https://www.terracloud.de/).
Ferner hat die Firma Sigma-IT GmbH einen Hauptsitz (71634 Ludwigsburg) und eine Niederlassung (88696 Owingen).

3 Vertraulichkeit

3.1 Zutrittskontrolle

3.1.1 Technische Maßnahmen

3.1.1.1 Ludwigsburg

Alarmanlage	Nicht vorhanden
Automatisches Zugangskontrollsystem	Nicht vorhanden
Biometrische Zugangssperren	Nicht vorhanden
Chipkarten / Transponder-Schließsysteme	vorhanden
Manuelles Schließsystem	vorhanden
Sicherheitsschlösser	vorhanden
Schließsystem mit Codesperre	Nicht vorhanden
Absicherung der Gebäudeschächte	Nicht vorhanden
Türen mit Knauf Außenseite	Nicht vorhanden
Klingelanlage mit Kamera	Nicht vorhanden

Videoüberwachung der Zugänge	vorhanden

3.1.1.2 Owingen

Alarmanlage	Nicht vorhanden
Automatisches Zugangskontrollsystem	Nicht vorhanden
Biometrische Zugangssperren	Nicht vorhanden
Chipkarten / Transponder-Schließsysteme	Nicht vorhanden
Manuelles Schließsystem	vorhanden
Sicherheitsschlösser	vorhanden
Schließsystem mit Codesperre	Nicht vorhanden
Absicherung der Gebäudeschächte	Nicht vorhanden
Türen mit Knauf Außenseite	vorhanden
Klingelanlage mit Kamera	Nicht vorhanden
Videoüberwachung der Zugänge	Nicht vorhanden

3.1.2 Organisatorische Maßnahmen

3.1.2.1 Ludwigsburg

Schlüsselregelung / -liste	vorhanden
Besucherregelung, z.B.	
- Empfang / Rezeption / Pförtner	vorhanden
- Besucherbuch / Protokoll der Besucher	Nicht vorhanden
- Mitarbeiter- / Besucherausweise	Nicht vorhanden
- Besucher in Begleitung durch Mitarbeiter	vorhanden
Sorgfalt bei Auswahl des Wachpersonals	Nicht vorhanden
Sorgfalt bei Auswahl Reinigungsdienst	vorhanden
Geheimhaltungsvereinbarungen (NDA) mit Wachpersonal/ Reinigungsdienst	nicht vorhanden

3.1.2.2 Owingen

Schlüsselregelung / -liste	vorhanden
Besucherregelung, z.B.	
- Empfang / Rezeption / Pförtner	Nicht vorhanden
- Besucherbuch / Protokoll der Besucher	Nicht vorhanden
- Mitarbeiter- / Besucherausweise	Nicht vorhanden
- Besucher in Begleitung durch Mitarbeiter	vorhanden
Sorgfalt bei Auswahl des Wachpersonals	Nicht vorhanden
Sorgfalt bei Auswahl Reinigungsdienst	Nicht vorhanden
Geheimhaltungsvereinbarungen (NDA) mit Wachpersonal/ Reinigungsdienst	Nicht vorhanden

3.2 Zugangskontrolle

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

3.2.1 Technische Maßnahmen

Login mit Benutzername + Passwort	vorhanden
Login mit biometrischen Daten	Nicht vorhanden
Anti-Viren-Software Server/ Clients	vorhanden
Anti-Virus-Software mobile Geräte	vorhanden
Firewall	vorhanden
Intrusion Detection Systeme (IDS)	vorhanden
Mobile Device Management	vorhanden
Einsatz VPN bei Remote-Zugriffen	vorhanden
Verschlüsselung von Mobilgeräten (Notebooks/ Tablet/	vorhanden
Verschlüsselung von mobilen Datenträgern	vorhanden
Gehäuseverriegelung	Nicht vorhanden
BIOS Schutz	Nicht vorhanden
Sperre externer Schnittstellen	Nicht vorhanden
Automatische Desktopsperre	vorhanden

3.2.2 Organisatorische Maßnahmen

Verwalten von Benutzerberechtigungen (Vergabe, Änderung und Entzug)	vorhanden
Benutzerberechtigungskonzept	vorhanden
Erstellen von Benutzerprofilen	vorhanden
Zentrale Passwortvergabe	vorhanden
Passwort-Richtlinie	vorhanden
Richtlinie „Löschen / Vernichten“	vorhanden
Richtlinie „Clean Desk“	vorhanden
Datenschutz-Richtlinie	vorhanden
Informationssicherheits-Richtlinie	vorhanden
Mobile Device Policy	vorhanden
Anweisung „Manuelle Desktopsperre“	vorhanden
Sorgfältige Auswahl und Überprüfung von Dienstleistern, die in Kontakt mit personen-bezogenen Daten gelangen	vorhanden

3.3 Zugriffskontrolle

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

3.3.1 Technische Maßnahmen

Akten-Schredder (DIN 66399: mind. Stufe P4 cross cut)	vorhanden
Physische Löschung/ Vernichtung von Datenträgern	vorhanden
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	vorhanden
Sichere Aufbewahrung von Datenträgern	vorhanden

3.3.2 Organisatorische Maßnahmen

Einsatz Berechtigungskonzepte	vorhanden
Anzahl an Administratoren auf das Notwendigste beschränkt	vorhanden
Datenschutztresor	Nicht vorhanden
Verwaltung Benutzerrechte durch Administratoren	vorhanden
Einsatz eines geprüften externer Datenvernichtungs-Dienstleisters	vorhanden

3.4 Trennungskontrolle

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

3.4.1 Technische Maßnahmen

Trennung von Produktiv- und Testumgebung	vorhanden
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	vorhanden
Mandantenfähigkeit relevanter Anwendungen	vorhanden

3.4.2 Organisatorische Maßnahmen

Steuerung über Berechtigungskonzept	vorhanden
Festlegung von Datenbankrechten	vorhanden
Datensätze sind mit Zweckattributen versehen	vorhanden
Es ist sichergestellt, dass Daten, die zu verschiedenen Zwecken verarbeitet werden, getrennt voneinander verarbeitet werden.	vorhanden
Es ist sichergestellt, dass Daten verschiedener Kunden getrennt voneinander verarbeitet werden.	vorhanden
Der Zugriff von Kunden auf Daten anderer Kunden ist ausgeschlossen.	vorhanden

4 Pseudonymisierung

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

4.1.1 Technische Maßnahmen

Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	vorhanden

4.1.2 Organisatorische Maßnahmen

Pseudonymisierung von Daten im Einsatz	vorhanden
Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/ pseudonymisieren	vorhanden
Verschlüsselung von Daten im Einsatz	vorahnden

5 Integrität

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

5.1 Weitergabekontrolle

5.1.1 Technische Maßnahmen

E-Mail-Verschlüsselung	vorhanden
Einsatz von VPN	vorhanden
Protokollierung der Zugriffe und Abrufe	vorhanden
Sichere Transportbehälter	vorhanden
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	vorhanden
Nutzung von Signaturverfahren	vorhanden

5.1.2 Organisatorische Maßnahmen

Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen	vorhanden
Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen	vorhanden
Weitergabe in anonymisierter oder pseudonymisierter Form	Wenn möglich vorhanden
Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen	vorhanden
Persönliche Übergabe mit Protokoll	Wenn benötigt vorhanden
Sichere Löschung von Daten nach Beendigung von Aufträgen	vorhanden
Dokumentation von Löschungsvorgängen	vorhanden

5.2 Eingabekontrolle

5.2.1 Technische Maßnahmen

Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	vorhanden
Manuelle oder automatisierte Kontrolle der Protokolle	vorhanden

5.2.2 Organisatorische Maßnahmen

Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können	vorhanden
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)	vorhanden

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	vorhanden
Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden	vorhanden
Klare Zuständigkeiten für Löschungen	vorhanden

6 Verfügbarkeit und Belastbarkeit

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

6.1 Verfügbarkeitskontrolle

6.1.1 Technische Maßnahmen

Feuer- und Rauchmeldeanlagen	TerraCloud, vorhanden
Feuerlöscher im Serverraum	TerraCloud, vorhanden
Serverraumüberwachung Temperatur und Feuchtigkeit	TerraCloud, vorhanden
Serverräume klimatisiert	TerraCloud, vorhanden
Unterbrechungsfreie Stromversorgung (USV) für Serversysteme	TerraCloud, vorhanden
Schutzsteckdosenleisten Serverraum	TerraCloud, vorhanden
Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quell-dichtung etc.)	TerraCloud, vorhanden
RAID System / Festplattenspiegelung	TerraCloud, vorhanden
Videoüberwachung Serverraum	TerraCloud, vorhanden
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	TerraCloud, vorhanden

https://www.wortmann.de/de-ch/content/unternehmen-zertifizierung.aspx
https://www.wortmann.de/de-at/content/cloud-detail.aspx

6.1.2 Organisatorische Maßnahmen

Backup & Recovery-Konzept (schriftlich ausformuliert)	vorhanden
Kontrolle des Sicherungsvorgangs	vorhanden, RMM
Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse.	Nicht vorhanden
Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums	Nicht notwendig (Georedundanz)
Verschlüsselung von Datensicherungen	vorhanden
Keine sanitären Anschlüsse im oder oberhalb des Serverraums	TerraCloud, vorhanden
Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)	Nicht vorhanden
Getrennte Partitionen für Betriebssysteme und Daten	

7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Diese Maßnahmen gelten für Ludwigsburg und Owingen.

7.1 Datenschutz-Management

7.1.1 Technische Maßnahmen

Software-Lösungen für Datenschutz-Management im Einsatz	Nicht vorhanden
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	vorhanden
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	Nicht vorhanden, im Aufbau Zertifizierung nach ISO 27001 ist angestrebt
Anderweitiges dokumentiertes Sicherheits- Konzept	vorhanden
Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Vorhanden, ISMS Team
Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Vorhanden, ISMS Team

7.1.2 Organisatorische Maßnahmen

Externes Team aus Datenschutzbeauftragten (DSB) bestellt	vorhanden
Internes Datenschutz-Team aus Datenschutz-Koordinatoren (DSK) bestellt.	vorhanden
Datenschutzmanagementsystem (DSMS) implementiert	vorhanden, dem ISMS angegliedert
Eine Leitlinie für Datenschutz und Informationssicherheit bezeugt die Übernahme der Verantwortung der Unternehmensleitung.	vorhanden
Richtlinien und Anweisungen für Beschäftigte zum Umgang mit personenbezogenen Daten	vorhanden
Regelmäßige Sensibilisierung der Mitarbeiter: Mindestens jährlich	vorhanden
Schulungs-Dokumentation	vorhanden
Mitarbeiter auf Vertraulichkeit verpflichtet	vorhanden, Arbeitsvertrag
Interner / externer Informationssicherheits- Beauftragter bestellt	vorhanden, intern
Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	Ja.
Die Organisation kommt den Informationspflichten nach Art. 13 und 14 EU-DSGVO nach	Ja.
Formalisierter Prozess zur fristgemäßen Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden	vorhanden
Meldewege bei Datenpannen	vorhanden
Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 EU-DSGVO	vorhanden

Periodische Überprüfung eingeräumter Berechtigungen.	vorhanden
Regelmäßige Überprüfung der Benutzerrollen und damit einhergehenden Berechtigungen.	vorhanden
Regelmäßige Kontrolle der Erreichbarkeit des Datenschutz-Teams	vorhanden

7.2 Incident-Response Management

7.2.1 Technische Maßnahmen

Einsatz von Firewall und regelmäßige Aktualisierung	vorhanden
Einsatz von Spamfilter und regelmäßige Aktualisierung	vorhanden
Einsatz von Virenscanner und regelmäßige Aktualisierung	vorhanden
Intrusion Detection System (IDS)	vorhanden
Intrusion Prevention System (IPS)	vorhanden
Darüber hinausreichende Maßnahmen (XDR)	vorhanden

7.2.2 Organisatorische Maßnahmen

Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)	vorhanden, ISMS-Team
Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	vorhanden
Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen	vorhanden
Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem	vorhanden, ISMS-Tickets
Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	vorhanden

7.3 Datenschutzfreundliche Voreinstellungen

7.3.1 Technische Maßnahmen

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

7.3.2 Organisatorische Maßnahmen

Einweisung der Mitarbeiter	vorhanden
Anweisungen für die Mitarbeiter	vorhanden

7.4 Auftragskontrolle (Outsourcing an Dritte)

7.4.1 Organisatorische Maßnahmen

Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation	vorhanden
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade im Bezug auf Datenschutz und Datensicherheit)	vorhanden
Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln	vorhanden
Schriftliche Weisungen an den Auftragnehmer	vorhanden
Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit	vorhanden
Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht	vorhanden
Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer	vorhanden
Regelung zum Einsatz weiterer Subunternehmer	vorhanden
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	vorhanden
Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus	vorhanden

1 Anlage 3: Liste der Ansprechpartner (Stand: 17.01.2023)

Gemäß Ziffer 11 der AVDI benennen die Parteien wechselseitig Ansprechpartner und werden diesbezügliche Änderungen dem jeweils anderen Vertragspartner unverzüglich schriftlich mitteilen.

Der Auftragnehmer meldet folgende Ansprechpartner:

Geschäftsführung	Martin Meier, Pascal Schmelzle
Externer DSB	Thomas Ströbele
Interner DSK	Pascal Schmelzle
Interner DSK	Madeleine Gasser

Die Ansprechpartner sind unter der Adresse des Auftragnehmers bzw. der Mailadresse datenschutz@sigma-it.de erreichbar.

Der Auftraggeber meldet folgende Ansprechpartner:

Fachbereich	Name	Telefon	E-Mail	Weisungsbefugnis

Erklärung: Die oben genannten Ansprechpartner sind die aktuell einzigen des Meldenden. Ältere Ansprechpartner-Listen verlieren hiermit Ihre Gültigkeit.

1 Anlage 4: Liste der Subunternehmer/Unterauftragnehmer (Stand: 17.01.2023)

Gemäß Ziffer 13 der AVDI meldet der Auftragnehmer hiermit folgende Subunternehmer, welche er zur Erfüllung seiner sich aus dieser Auftragsverarbeitung ergebenden vertraglich vereinbarten Leistung unterbeauftragt. Änderungen werden schriftlich mitgeteilt:

Subunternehmer	Anschrift	Leistungsteil
DocuWare		3rd-Level Support
Jobrouter		3rd-Level Support
topfact		3rd-Level Support
Tanss		3rd-Level Support

Zusätzlich setzt Auftragnehmer im Bedarfsfall weitere Auftragnehmer ein, die aufgrund der Varianz nicht einzeln spezifiziert werden können. Dies sind insbesondere:

Subunternehmer	Leistungsteil
TerraCloud	Backup, IaaS, SaaS, MIaas, Firewall-aaS,
Sophos	Managed Endpoint Protection
Hornet	Antispam, AV, E-Mail-Archivierung
DocuWare	Cloud Lösungen (Azur RZ)
WOASI	RMM Meldungen in Ticketsystem Übertragen (Hetzner RZ)
Hetzner	Webseite, DNS
Microsoft	O365, Lizenzen, SW-Lösungen
Starface	VoIP Lösungen on Premises/Cloud
Fördermittel	Prüfung von Anträgen für Bundesbehörden (z.B. Euronorm GmbH)
Datev	3rd-Level Support, Vergabe von Sicherheitskomponenten
Wortmann	Lizenzen, HW allgemein
Riverbird	RMM System (Inventarisierung, Patchmanagement, Überwachung …)
Servereye	Überwachung von Systemsensoren

In Notfällen, die es dem Auftragnehmer unmöglich machen, seine vertraglichen Leistungen zu erfüllen oder wenn Gefahr im Verzug ist, welche die Schutzziele des Datenschutzrechts wesentlich bedrohen und es im eigenen Interesse des Auftraggebers ist, kann der Auftragnehmer kurzfristig weitere Subunternehmer hinzuziehen, um den Notfall abzuwenden oder zu bewältigen.

Erklärung: Die oben genannten Subunternehmer sind die aktuell einzigen betroffenen des Auftragnehmers. Ältere Subunternehmer-Listen verlieren hiermit Ihre Gültigkeit.

1 Anlage 5: Meldeformular für Datenschutzvorfälle (Stand: 17.01.2023)

Dieses Dokument dient dem Auftraggeber Vorfälle zu dokumentieren, bei denen der Verdacht besteht, dass sie Daten-schutzvorfälle im Sinne von Art. 33 EU-DSGVO sein könnten. Soweit die damit verbundenen Verarbeitungen den Auftrag-nehmer betreffen, ist dieser ggf. auch zu informieren.

1. Allgemeine Angaben zum Vorfall

Feststellung des Vorfalls (Datum, Uhrzeit):

Zeitpunkt des Vorfalls, betroffener Zeitraum:
Datenverarbeitungsverfahren:
Verantwortlicher Fachbereich:
Verantwortlicher Bearbeiter für den Vorfall:

1.1 Betroffene Systeme/Objekte:
Wie hat sich der Vorfall ereignet?
Welche Folgen wurden festgestellt?

1.2 Reaktionen und Zustand des Systems
Erste Reaktionen/Maßnahmen:
Aktueller Zustand des Systems:

2. Angaben zum Vorfall

2.1 Art des Vorfalls:
(Vorfälle sind z. B. Verlust der Vertraulichkeit, Datendiebstahl, Zerstörung oder Verfälschung der Daten, Übermittlung an unbefugte Stellen etc.)

2.2 Betroffene Personengruppen:

2.3 Zahl der betroffenen Personen:

2.4 Kategorien von personenbezogenen Daten:

2.5 Wahrscheinliche Folgen/Risiken der Verletzung des Schutzes personenbezogener Daten:
(Hier sind die möglichen Risiken und Folgen für die Betroffenen anzugeben.)

3. Eingeleitete Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

3.1 Eingerichtete Maßnahmen:
(Hier sind die Maßnahmen zu beschreiben, die zum Schutz der personenbezogenen Daten gegen Vorfälle dieser Art ein-gerichtet worden sind.)

3.2 Weitere beabsichtigte Maßnahmen:
(Hier sind die Maßnahmen zu beschreiben, deren Einrichtung aufgrund des Vorfalls zusätzlich noch geplant ist.)

1 Anlage 6: Ergänzende Regelungen zum Austausch von Datenträgern und Fernwartung (Stand: 17.01.2023)

1.1 Austausch von Datenträgern oder von Geräten mit Datenträgern

(1) Werden durch den Auftragnehmer bei einer Reparatur oder Wartung Datenträger mit möglicherweise personenbezogenen oder sonstigen vertraulichen Daten ausgetauscht oder Geräte mit derartigen Datenträgern zurückgenommen, ist der Auftraggeber zu verständigen. Die ausgetauschten Datenträger sind dem Auftraggeber auszuhändigen oder in Ab-stimmung mit dem Auftraggeber physisch zu vernichten oder sicher zu löschen. Eine Entfernung und Mitnahme von Datenträgern ohne Einwilligung des Auftraggebers ist unzulässig.
(2) Das Löschverfahren ist dem Auftraggeber darzulegen und die sichere Löschung bzw. Vernichtung der Datenträger ist vom Auftragnehmer zu bestätigen. Die Löschung ist durch sicheres Überschreiben (z.B. BSI-Richtlinie zum Geheimschutz von Verschlusssachen beim Einsatz von IT (VSITR) oder Standard 5220.22-M des US Verteidigungsministeriums oder nach DIN 33858 – Löschung magnetischer Datenträger) durchzuführen.

1.2 Durchführung der Fernwartung

Werden Auftragsleistungen im Wege der Fernwartung durchgeführt, gelten zusätzlich folgende Vereinbarungen:
(1) Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Die Fernwartung erfolgt, soweit möglich, ohne gleichzeitige Speicherung von Da-ten.
(2) Der Auftragnehmer muss personenbezogene Daten, die er bei der Fernwartung erhalten oder gewonnen hat, unverzüglich sicher löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind. Etwaige dem Auftragnehmer übergebene Papierausdrucke oder sonstige Datenträger mit personenbezogenen oder sonstigen vertraulichen Daten sind dem Auftragnehmer nach Abschluss der Fernwartungsarbeiten unverzüglich zurückgeben oder sicher zu vernichten.
(3) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen, Ausnahmen sind mit dem Auftraggeber abzustimmen.
(4) Der Beginn der Fernwartung ist vom Auftragnehmer anzukündigen, um dem Auftraggeber die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen. Ggf. entstehende Kosten übernimmt der Auftraggeber. Die Mitarbeiter des Auftragnehmers verwenden nach dem Stand der Technik hinreichend sichere Identifizierungs- und Einwahlverfahren. Die Fernwartung darf nur über nach dem Stand der Technik sichere Leitungen abgewickelt werden.
(5) Der Auftragnehmer verpflichtet sich, nur zur Vertragserfüllung, auf Grund von Störungsmeldungen oder auf Grund sonstiger ausdrücklicher Anforderungen des Auftraggebers mittels Fernwartung bzw. Remote-Zugriff auf Systeme, Soft-ware und Daten zuzugreifen und danach dem Auftraggeber Serviceberichte zu erstellen.
(6) Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen (sofern technisch möglich). Beide Parteien sind berechtigt, die Fernwartungsaktivitäten zu protokollieren, die Protokolle zu über-prüfen und eine angemessene Zeit aufzubewahren.
(7) Wird die Fernwartung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Serviceleistung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung von der Wartungszentrale aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.
(8) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, wenn der Auftragnehmer von den vereinbarten Sicherheitsmaßnahmen abweicht oder die Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten durchgeführt wird