Auftragsverarbeitungsvereinbarung

Auftragnehmer

opta data IT Solutions GmbH
Berthold-Beitz-Boulevard 514
45141 Essen
- im folgenden odITS genannt -

1. Gegenstand und Dauer des Auftrags

- Gegenstand
  Der Auftragnehmer als Dienstleistungsunternehmen und Systemhaus übernimmt für den Auftraggeber folgende in der Anlage 2 aufgeführten Tätigkeiten.

- Dauer
  Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der entsprechenden Leistungsvereinbarung(en) und ist an diese gekoppelt.

2. Konkretisierung des Auftragsinhalts

- Art und Zweck der vorgesehenen Verarbeitung von Daten:
  Der Umfang der Tätigkeiten des Auftragnehmers richtet sich nach den Anforderungen des Auftraggebers. Die Beschreibung und die Art der Datenverarbeitung ergibt sich aus der Anlage 2 zu dieser Auftragsverarbeitung und basiert auf der in Anlage 1 gewählten Produkte. Diese Vereinbarung zur Auftragsverarbeitung (AV-Vereinbarung) entspricht den rechtlichen Anforderungen der Artt. 28, 29 DSGVO, des § 80 SGB X sowie der § 29 KDG, § 29 KDR-OG und §30 DSG-EKD, wenn es sich um einen kirchlichen Auftraggeber handelt.

- 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.

- Der Auftragnehmer ist berechtigt, Daten in anonymisierter Form auch für andere Zwecke wie etwa Marktanalysen zu verwenden.

- Art der Daten
  Die personenbezogenen Datenarten/-kategorien ergeben sich aus der Anlage 2 dieser AV-Vereinbarung.

- Kategorien betroffener Personen
  Die Kategorien der durch die Verarbeitung betroffenen Personen ergeben sich aus der Anlage 2 dieser AV-Vereinbarung.

3. Technisch-organisatorische Maßnahmen

- 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.
- Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Äquivalent gelten die §§ 5, 26 KDG. 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.
- 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

- 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.
- 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:

- Schriftliche Bestellung, soweit nach DSGVO bzw. BDSG-Neu erforderlich, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
- Dessen Kontaktdaten werden ggf. dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird ggf. dem Auftraggeber unverzüglich mitgeteilt.
- Dessen jeweils aktuelle Kontaktdaten sind ggf. auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- 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 und für die Fälle der Einbeziehung des § 203 StGB in das Vertragsverhältnis auf die Schweigepflicht nach § 203 StGB 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.
- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

- 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.
- Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
- Der Auftraggeber stimmt den in der Anlage 2 aufgeführten Unterauftragnehmern je nach der in der Anlage 1 aufgeführten Dienstleistungen bzw. Produkten zu.
- Die Beauftragung der Unterauftragnehmer erfolgt unter den Bedingungen einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 DSGVO.

  Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- Der Auftragnehmer über eine solche geplante Auslagerung auf Unterauftragnehmer den Auftraggeber innerhalb einer angemessenen Zeit vorab schriftlich oder in Textform informiert und Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt.
- In Notfällen, die den Ablauf des Auftrags behindern würden oder die Verarbeitung zum Erliegen bringen könnten, darf der Auftragnehmer ohne vorherige Zustimmung einen Unterauftragnehmer wechseln. Dabei sind die Bedingungen der Artt. 28, 29 und 32 DSGVO zu beachten. Der Wechsel muss dem Auftraggeber innerhalb einer Woche schriftlich oder in Textform mitgeteilt werden. Der Wechselgrund muss durch den Auftragnehmer in nachvollziehbarer Weise dokumentiert werden.
- Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- 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.
- Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung des Auftraggebers sowie des Hauptauftragnehmers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.
- Dem Einsatz von Mitarbeitern des Auftragnehmers in Heimarbeit oder im Home-Office stimmt der Auftraggeber zu.

7. Kontrollrechte und Pflichten des Auftraggebers

- 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.
- 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.
- 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 oder DIN-ISO 27001).
  - Der Auftragnehmer ermöglicht dem Auftraggeber nach vorheriger Terminabsprache jährliche Kontrollen. Für die Ermöglichung von Kontrollen, die über dieses Maß hinaus gehen, kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Dieser darf die tatsächlich entstandenen Kosten nicht überschreiten.
  - Der Auftraggeber hat seinen Pflichten gegenüber dem Betroffenen gemäß Art. 13 DSGVO nachzukommen und dem Betroffenen mitzuteilen, dass der Auftragnehmer und die einbezogenen Unterauftragnehmerin die Verarbeitung seiner personenbezogenen Daten involviert sind. Insofern verpflichtet sich der Auftraggeber zur Einhaltung und Umsetzung seiner Pflichten nach der EU-DSGVO. Ferner ist der Auftraggeber verpflichtet, sofern er Berufsgeheimnisträger ist, ggfs. eine Schweigepflichtentbindungserklärung des Betroffenen einzuholen. Diese hat er dem Auftragnehmer auf Anfrage (Stichprobenprüfung) zur Verfügung zu stellen. Etwas anderes gilt dann, wenn er den Auftragnehmer wirksam nach § 203 Abs. 4 S. 1 StGB verpflichtet hat.

8. Mitteilung bei Verstößen des Auftragnehmers

- Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
  - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
  - 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
  - die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
  - die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind und die nicht Bestandteil der Pflichten eines Auftragnehmers im Rahmen der DSGVO sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

- Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Schriftform.
- 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

- 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.
- 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. Ausgenommen von dieser Regel sind Daten, die der Auftragnehmer zur Wahrung der gesetzlichen Aufbewahrungsfristen nicht löschen darf.
- Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertrags-ende dem Auftraggeber übergeben.

11. Sonstiges

- Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vereinbarungsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.
- Sollten sich datenschutzrechtliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.
- Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.
- Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der personenbezogenen Daten/Sozialdaten und der zugehörigen Datenträger ausgeschlossen.
- Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.

12. Inkrafttreten

- Diese Datenschutzbestimmungen treten mit Inkrafttreten der Leistungsvereinbarung in Kraft.
- Gerichtsstand entspricht dem des Auftraggebers in dessen AGB.

Anlage – Technische und organisatorische Maßnahmen

Eine Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO ist Bestandteil dieses Auftrags und liegt dieser Vereinbarung als Anlage 3 bei. Diese zum Datenschutz getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert.

(Ende der Vereinbarung zur Auftragsverarbeitung)

Anlage 1

Produktübersicht opta data IT Solutions GmbH
(Stand 02/2024)

Lfd.-Nr.	Produktname
1	od | care Konkretisierung der Produktangaben in Anlage 2 auf Seite 5
2	od | care mobile Konkretisierung der Produktangaben in Anlage 2 auf Seite 6
3	eva/3 viva! ambulant Konkretisierung der Produktangaben in Anlage 2 auf Seite 7
4	eva 3 office Konkretisierung der Produktangaben in Anlage 2 auf Seite 8
5	eva 3 careplan Konkretisierung der Produktangaben in Anlage 2 auf Seite 9
6	meine Tour Konkretisierung der Produktangaben in Anlage 2 auf Seite 10
7	iDokument Konkretisierung der Produktangaben in Anlage 2 auf Seite 11

Anlage 2

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Produkt	od | care
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber konkret folgende Tätigkeiten: • Bereitstellung einer Webapplikation (od | care ambulant) • Bereitstellung ein Hosting-Umgebung (od | care Hosting) • Bereitstellung einer Android- und iOS-App (od | care mobile) • Bereitstellung Datenaustausch zwischen den Anwendungen • Wartung der Anwendungen • Support für die Anwendungen • Datensicherung der Web- und Hosting-Umgebung
Art der Daten	Kundendaten: • Adressdaten • Vertragsstammdaten • Kontakt- / Kommunikationsdaten • Rechnungsdaten Patientendaten des Kunden (Betroffene im Sinne der DSGVO): • Adressdaten • Kontakt- / Kommunikationsdaten • Geburtsdatum • Staatsangehörigkeit • Geschlecht • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • Versichertendaten • zuständigen Ärzte • Rechnungsdaten • Zahlungsdaten • Kundenhistorie
Kategorie Betroffener	• Kunden • Lieferanten • Interessenten • Beschäftigte • Ansprechpartner • Patienten (gesetzlich und privat Versicherte – betroffene Personen im Sinne des Art. Nr. 1 DSGVO)
Unterauftragnehmer	Beschreibung
	SIEDA Systemhaus für Intelligente EDV-Anwendungen GmbH, 67663 Kaiserslautern (Erbringung von Support-, Beratungs- und Schulungsdienstleistungen)
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	opta data IT GmbH, 45141 Essen (Bereitstellung Loginverfahren “Single-Sign-On“)
	opta data digital communications GmbH, 45141 Essen (Hosting und Bereitstellung des Matomo Server)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Produkt	od | care mobile
Konkretisierung des Auftragsinhalts	Die Anwendung ist nur in Kombination mit einer eva/3 viva! im Server-Hosting nutzbar. Der Auftragnehmer übernimmt für den Auftraggeber konkret folgende Tätigkeiten: • Bereitstellung einer Android- und iOS-App (od | care mobile) • Bereitstellung Datenaustausch zwischen den Anwendungen • Wartung der Anwendungen • Support für die Anwendungen • Datensicherung der Web- und Hosting-Umgebung
Art der Daten	Kundendaten: • Adressdaten • Vertragsstammdaten • Kontakt- / Kommunikationsdaten Patientendaten des Kunden (Betroffene im Sinne der DSGVO): • Adressdaten • Kontakt- / Kommunikationsdaten • Geburtsdatum • Staatsangehörigkeit • Geschlecht • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • Versichertendaten • zuständigen Ärzte • Rechnungsdaten • Zahlungsdaten • Kundenhistorie
Kategorie Betroffener	• Kunden • Lieferanten • Interessenten • Beschäftigte • Ansprechpartner • Patienten (gesetzlich und privat Versicherte – betroffene Personen im Sinne des Art. Nr. 1 DSGVO)
Unterauftragnehmer	Beschreibung
	SIEDA Systemhaus für Intelligente EDV-Anwendungen GmbH, 67663 Kaiserslautern (Erbringung von Support-, Beratungs- und Schulungsdienstleistungen)
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	opta data IT GmbH, 45141 Essen (Bereitstellung Loginverfahren “Single-Sign-On“)
	opta data digital communications GmbH, 45141 Essen (Hosting und Bereitstellung des Matomo Server)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Produkt	eva/3 viva! ambulant
Konkretisierung des Auftragsinhalts	Der Auftragnehmer schaltet sich über das Internet mit Hilfe der Standardsoftware TeamViewer auf einen PC des Auftragnehmers auf und nimmt dort Reparaturarbeiten in der Branchenlösung vor. Die Freischaltung durch den Auftraggeber erfolgt mit Hilfe einer telefonisch übermittelten Fernsteuerungs-ID. Der Auftragnehmer hat die Möglichkeit die Sitzung zu überwachen. In Ausnahmefällen kann es auch vorkommen, dass der Auftragnehmer eine komplette Datenbank zu Analysezwecken überspielen muss. Nach der Analyse werden die Daten unverzüglich beim Auftragnehmer gelöscht. Ferner spielt der Auftragnehmer Updates, Patches oder neu Programmstände ein. Dies geschieht immer in Absprache mit dem Auftraggeber. Der Auftragnehmer übernimmt für den Auftraggeber konkret folgende Tätigkeiten: • Bereitstellung der Serverumgebung im Rechenzentrum der opta data (nur bei Server-Hosting) • Fernwartung und Reparatur der Branchenlösung / Applikation • Fernwartung und Reparatur von Datenbanken auf die die Branchenlösung zugreift • Einspielen von Updates und Patches zur Behebung von Fehlern in die Branchenlösung • Einspielen neuer Programmständen • Sicherstellen der Datensicherung (nur bei Server-Hosting)
Art der Daten	• Adressdaten • Vertragsstammdaten • Kontakt- / Kommunikationsdaten • Geburtsdatum • Staatsangehörigkeit • Geschlecht • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • Versichertendaten • zuständigen Ärzte • Rechnungsdaten • Zahlungsdaten • Kundenhistorie • IP-Adressen • GPS-Daten von Fahrzeugen (nur bei eva/3 geo tracking)
Kategorie Betroffener	• Kunden • Lieferanten • Interessenten • Mitarbeiter • Ansprechpartner • Patienten (gesetzl. und privat Versicherte – betroffene Personen im Sinne des Art. Nr. 1 DSGVO)
Unterauftragnehmer	Beschreibung
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	PTV Planung Transport Verkehr AG, 76131 Karlsruhe (Softwareanbieter des GEO Servers)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Produkt	eva 3 office
Konkretisierung des Auftragsinhalts	Der Auftragnehmer schaltet sich über das Internet mit Hilfe der Standardsoftware TeamViewer auf einen PC des Auftragnehmers auf und nimmt dort Reparaturarbeiten in der Branchenlösung vor. Die Freischaltung durch den Auftraggeber erfolgt mit Hilfe einer telefonisch übermittelten Fernsteuerungs-ID. Der Auftragnehmer hat die Möglichkeit die Sitzung zu überwachen. In Ausnahmefällen kann es auch vorkommen, dass der Auftragnehmer eine komplette Datenbank zu Analysezwecken überspielen muss. Nach der Analyse werden die Daten unverzüglich beim Auftragnehmer gelöscht. Ferner spielt der Auftragnehmer Updates, Patches oder neu Programmstände ein. Dies geschieht immer in Absprache mit dem Auftraggeber. Der Auftragnehmer übernimmt für den Auftraggeber konkret folgende Tätigkeiten: • Bereitstellung der Serverumgebung im Rechenzentrum der opta data (nur bei Server-Hosting) • Fernwartung und Reparatur der Branchenlösung / Applikation • Fernwartung und Reparatur von Datenbanken auf die die Branchenlösung zugreift • Einspielen von Updates und Patches zur Behebung von Fehlern in die Branchenlösung • Einspielen neuer Programmständen • Sicherstellen der Datensicherung (nur bei Server-Hosting)
Art der Daten	• Adressdaten • Vertragsstammdaten • Kontakt- / Kommunikationsdaten • Geburtsdatum • Staatsangehörigkeit • Geschlecht • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • Versichertendaten • zuständigen Ärzte • Rechnungsdaten • Zahlungsdaten • Kundenhistorie • IP-Adressen • GPS-Daten von Fahrzeugen (nur bei eva/3 geo tracking)
Kategorie Betroffener	• Kunden • Lieferanten • Interessenten • Mitarbeiter • Ansprechpartner • Patienten (gesetzl. und privat Versicherte – betroffene Personen im Sinne des Art. Nr. 1 DSGVO)
Unterauftragnehmer	**Beschreibung**
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	PTV Planung Transport Verkehr AG, 76131 Karlsruhe (Softwareanbieter des GEO Servers)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Zur ständigen Verbesserung unserer Software verwenden wir das Analysetool Matomo. Dazu werden Cookies gesetzt. Durch Anonymisierung der IP-Adressen und TTDSG und DSGVO konforme Verwendung von Matomo ist ein Rückschluss auf einzelne User nicht möglich

Produkt	eva 3 careplan
Konkretisierung des Auftragsinhalts	Der Auftragnehmer schaltet sich über das Internet mit Hilfe der Standardsoftware TeamViewer auf einen PC des Auftragnehmers auf und nimmt dort Reparaturarbeiten in der Branchenlösung vor. Die Freischaltung durch den Auftraggeber erfolgt mit Hilfe einer telefonisch übermittelten Fernsteuerungs-ID. Der Auftragnehmer hat die Möglichkeit die Sitzung zu überwachen. In Ausnahmefällen kann es auch vorkommen, dass der Auftragnehmer eine komplette Datenbank zu Analysezwecken überspielen muss. Nach der Analyse werden die Daten unverzüglich beim Auftragnehmer gelöscht. Ferner spielt der Auftragnehmer Updates, Patches oder neu Programmstände ein. Dies geschieht immer in Absprache mit dem Auftraggeber. Der Auftragnehmer übernimmt für den Auftraggeber konkret folgende Tätigkeiten: • Bereitstellung der Serverumgebung im Rechenzentrum der opta data (nur bei Server-Hosting) • Fernwartung und Reparatur der Branchenlösung / Applikation • Fernwartung und Reparatur von Datenbanken auf die die Branchenlösung zugreift • Einspielen von Updates und Patches zur Behebung von Fehlern in die Branchenlösung • Einspielen neuer Programmständen • Sicherstellen der Datensicherung (nur bei Server-Hosting)
Art der Daten	• Adressdaten • Vertragsstammdaten • Kontakt- / Kommunikationsdaten • Geburtsdatum • Staatsangehörigkeit • Geschlecht • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • Versichertendaten • zuständigen Ärzte • Rechnungsdaten • Zahlungsdaten
Kategorie Betroffener	• Kunden • Lieferanten • Interessenten • Mitarbeiter • Ansprechpartner • Bewohner (gesetzl. und privat Versicherte – betroffene Personen im Sinne des Art. Nr. 1 DSGVO)
Unterauftragnehmer	Beschreibung
	SIEDA Systemhaus für Intelligente EDV-Anwendungen GmbH, 67663 Kaiserslautern (Erbringung von Support-, Beratungs- und Schulungsdienstleistungen)
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	opta data IT GmbH, 45141 Essen (Bereitstellung Loginverfahren “Single-Sign-On”)
	opta data digital communications GmbH, 45141 Essen (Hosting und Bereitstellung des Matomo Server)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Produkt	meine Tour
Konkretisierung des Auftragsinhalts	Der Auftragnehmer stellt dem Auftraggeber per Synchronisation die für den App-Betrieb benötigten Daten zur Verfügung. Die Synchronisation wird als Webservice für den Austausch der Daten zwischen der Hauptanwendung und der App, sowie von der App in Richtung Hauptanwendung zur Verfügung gestellt. Der Auftragnehmer erhält vom Auftraggeber eine individuelle Kennung je App, um die bereitgestellten Daten zwischen der App und der Hauptanwendung sowie umgekehrt austauschen zu können. Der Auftragnehmer übernimmt für den Auftraggeber konkret folgende Tätigkeiten: • Bereitstellung der Serverumgebung für die Datensynchronisation • Zur Verfügungstellung von Updates für die App • Einspielen von Updates und Servicepacks zur Behebung von Fehlern in der Hauptanwendung • Einspielen von neuen Programmständen zur Hauptanwendung (Erweiterung) • Sicherstellen der Datensicherung auf dem Server der Datensynchronisation
Art der Daten	• Adressdaten • Kontakt- / Kommunikationsdaten • Geburtsdatum • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • zuständigen Ärzte
Kategorie Betroffener	• Klienten • Ärzte • Bezugspersonen • Mitarbeiter • Lieferanten • Dienstpläne • Tourenpläne
Unterauftragnehmer	Beschreibung
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Konkretisierung des Auftragsinhalts
Art der Daten
Kategorien betroffener Personen
Unterauftragnehmer

Produkt	iDokument
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Zugang zur kundeneigenem Webportal („Webstand“) von iDokument für Administration/Wartung und Benutzer-/Lizenzverwaltung mit Auftraggeber eigenem Administrationszugang. Weiterhin schaltet sich der Auftraggeber für Fehlerprüfungen und setzen von Programmeinstellungen während telefonischer Absprache über ein Fernwartungstool bei bestehender Internetverbindung in die iDokument-App auf dem iPad auf. Diese Fernwartungsanfrage muss in der iDokument-App vom Auftraggeber explizit bestätigt werden, bevor die Aufschaltung möglich ist. • Benutzeradministration und Lizenzverwaltung (Onlineportal) Geburtsdatum • Administration von Systemeinstellungen wie z.B. Autoarchivierung von Patienten nach Rücksprache • Fernwartung zur Fehlerprüfung / Setzen von technischen Einstellungen der iDokument-App • Einspielung von Updates für die Weboberfläche in zuvor angekündigten Wartungsfenstern • Bereitstellung von neuen iDokument-App Versionen im Apple App Store Der Auftragsinhalt ist nicht abschließend. Je nach Wahl von Zusatzdienstleistungen durch den Auftraggeber bei dem Auftragnehmer, kann der Auftragsinhalt über die an dieser Stelle geregelten Inhalte hinausgehen. In diesem Fall ergibt sich eine weitere Konkretisierung aus der Leistungsvereinbarung. Der Auftragnehmer ist berechtigt, Daten in anonymisierter Form auch für andere Zwecke, wie etwa Nutzungsauswertungen zu verwenden.
Art der Daten	• Adressdaten • Geburtsdaten • Staatsangehörigkeit • Geschlecht • Vertragsstammdaten • Versichertendaten • Kontakt- / Kommunikationsdaten • Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO • Sozialdaten gem. § 67 Abs. 2 SGB X • Zuständige Ärzte • Angehörigendaten • Stammdaten von Kundenpartnern wie Pflegedienste oder Stationäre Einrichtungen
Kategorie Betroffener	• Kunden • Interessenten • Beschäftigte • Ansprechpartner • Patienten (gesetzlich und privat Versicherte – betroffene Personen im Sinne des Art. Nr. 1 DSGVO) • Kundenpartner (Pflegedienste, Einrichtungen)
Unterauftragnehmer	Beschreibung
	opta data Finance GmbH, 45141 Essen (Betreuung der IT-Infrastruktur, Nutzung der Serverräume)
	Microsoft Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)

Anlage 3

Aufstellung für Auftraggeber der opta data IT Solutions GmbH zu den bei der opta data IT Solutions GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz

Diese Auflistung der bei der opta data IT Solutions GmbH getroffenen technischen und organisatorischen Maßnahmen orientiert sich nach den „14 Geboten" im Datenschutz gem. § 64 BDSG (neu), § 78 a SGB X, § 26 KDG sowie Art. 32 DSGVO und soll es ermöglichen, dem Auftraggeber seine Prüf- und Dokumentationspflicht bei Auftragsdatenverarbeitung gem. Artt. 28 und 29 DSGVO, 80 SGB X und §§ 29, 30 KDG zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Artt. 28 und 29 DSGVO bzw. §§ 29 und 30 KDG konformen, Dienstleistungsvertrag gedacht und kann jedem Auftraggeber auf Anforderung zur Verfügung gestellt werden.

Ergänzend sei noch erwähnt, dass die opta data IT Solutions GmbH nach DIN/ISO 27001 zertifiziert ist und es IT-Notfallpläne, Datensicherungs- und Berechtigungskonzepte und dokumentierte Prozessabläufe gibt.

Die Daten, die bei der opta data IT Solutions GmbH im Auftrag verarbeitet werden, sind als besonders sensibel eingestuft. Es handelt sich um personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO und um Sozialdaten gemäß § 67 Abs. 1 SGB X in Verbindung mit besonderen Daten gemäß Art. 4 Nr. 15 DSGVO (Gesundheitsdaten).

Allgemeiner Teil

1. Name und Anschrift des Unternehmens

opta data IT Solutions GmbH,
Berthold-Beitz-Boulevard 514,
45141 Essen

2. Kontakt

Integrierte Managementsysteme / Bereich Datenschutz
Tel.: 0201 89094 -444; Fax: 0201 89094 -700
E-Mail: datenschutz@optadata.de

3. Name der Geschäftsführer

Alexander Boschuk, Christian Teufel

4. Datenschutzbeauftragter

Joachim Kramer
Datenschutz Kramer & Kramer GmbH
Elsternweg 24, 42555 Velbert
Tel.: 02052 92897 66; Fax: 02052 92897 67
E-Mail: j.kramer@datenschutz-kramer.de

Bestellung

- externer Datenschutzbeauftragter gem. § 4 f Abs. 2 BDSG bzw. Art.37 DSGVO und § 38 BDSG-neu
- schriftliche Bestellung vom 02.07.2019 liegt vor

Qualifikation

- Datenschutz-Auditor (TÜV) Zertifizierungsstelle für Personal TARZERT der TÜV Akademie Rheinland Nr. 19553
- über 23 Jahre Erfahrung im IT-Bereich
- regelmäßige Fortbildungen
- Mitglied im Erfa-Kreis für Datenschutzbeauftragte der Region MEO
- GDD Mitglied
- Die Firma Datenschutz Kramer & Kramer GmbH besitzt über 30 Jahre Erfahrung im Datenschutz

5. Informationssicherheits-Beauftragte nach DIN ISO/IEC 27001

Informationssicherheits-Beauftragter (IT)
Tobias Windhaus
- Auditor nach ISO/IEC 27001 (TÜV)
- schriftliche Ernennung liegt vor

Informationssicherheits-Beauftragter (Organisation)
Dirk Nienaber
- Auditor nach ISO/IEC 27001 (TÜV)
- schriftliche Ernennung liegt vor

6. Mitarbeiter der opta data IT Solutions GmbH

- Alle Mitarbeiter sind schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB und der Vertraulichkeit nach DSGVO und BDSG sowie zur Wahrung des Sozialgeheimnisses nach § 35 SGB I verpflichtet worden
- die Verpflichtung erfolgte auf einem extra Formular
- die der Verpflichtung zu Grunde liegenden Gesetzestexte wurden allen Mitarbeitern zugänglich gemacht
- die Verpflichtung wird bei Einstellung durch das Personalbüro der opta data Gruppe vorgenommen
- Betriebsvereinbarung über die private Nutzung von E-Mail, Internet und Telefon
- alle Mitarbeiter werden in regelmäßigen Abständen durch den bDSB geschult

7. Verzeichnis von Verarbeitungstätigkeiten

Das „Verzeichnis der Verarbeitungstätigkeiten" gem. Art. 30 DSGVO wird elektronisch geführt und ist in einem IMS-System dokumentiert.

Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen beinhalten zwei unterschiedliche Rechenzentrum Standorte. Unterschiede werden mit RZ-1 und RZ-2 dargestellt, wobei es sich bei RZ-1 um das Rechenzentrum der eva/3 Produktpalette handelt. Das Rechenzentrum RZ-2 beinhaltet die Anwendung iDokument.

Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)

RZ-1
- das gesamte Firmengelände ist mit einem 2m hohen Stahlzaun umgeben
- Zufahrt (Zutritt) nur über zwei, außerhalb der Geschäftszeitenverschlossenen, Stahltore
- Mitarbeiter und Besucher müssen während der Geschäftszeiten an der besetzten Rezeption vorbei
- außerhalb der Geschäftszeiten sind die Fenster der unteren Etagen sowie die Rezeption durch eine Alarmanlage gesichert
- mehrere Kameras überwachen das gesamte Firmengelände sowie die Eingänge, die Bilder werden auf 2 Monitore in der Rezeption übertragen und auf einem Festplattenrecorder 20 Tage lang gespeichert
- nachts kontrolliert ein Wachdienst regelmäßig das Gebäude
- jeder Mitarbeiter hat einen Firmenausweis (Codekarte), Besucher werden registriert und bekommen einen Gastausweis.
- Besucher werden an der Rezeption abgeholt und begleitet

RZ-2
- Closed-Shop-Betrieb
- Alle Gebäude werden per Video überwacht
- Die Serverräume werden automatisch per Video überwacht, sobald sie betreten werden.

- Der Zutritt in die Büroräume ist nur per RFID möglich.
- Besucher müssen sich an den Zentralen anmelden.
- Besucher- und Mitarbeiterausweise autorisieren den Zutritt.
- Die Zentrale im Berthold-Beitz-Boulevard 461 ist rund um die Uhr, an 7 Tagen in der Woche besetzt.
- Der Wachtdienst fährt außerhalb der Arbeitszeiten alle Standorte der Unternehmensgruppe in Essen regelmäßig an.
- Die Serverräume sind mit separaten Sicherheitsschlössern bzw. Zahlencode-Schlössern ausgestattet.
- Es kann nachvollzogen werden, welche Tür wann und von wem geöffnet wurde (Logfiles in den Türzutrittssystemen)

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

RZ-1
- Benutzername und Kennwort
- automatische Sperrung (Pausenschaltung)
- Sperrung des Accounts bei wiederholter Falschanmeldung
- datenschutzgerechte Passwortrichtlinien gem. BSI werden vom Domaincontroller vorgegeben
- Active Directory mit Zugangsprotokoll
- Server mit zusätzlichen Administrator Passwörtern
- Mitarbeiterprofile sind Rollen basierend
- Inventarisierte Hardware
- Daten in Papierform werden gesammelt und in abschließbaren Containern entsorgt, wenn die Container voll sind, werden sie von der Rhenus Data Office GmbH, Ratingen abgeholt und gemäß DIN 66399 P-4 datenschutzgerecht entsorgt (gegen Quittung)
- Einzelne Schriftstücke werden tagesaktuell mit einem Aktenvernichter der Sicherheitsstufe P-5 nach DIN 66399 vernichtet

RZ-2
- Daten in Papierform werden gesammelt und in abschließbaren Containern entsorgt. Wenn die Container voll sind, werden sie von der Rhenus Data Office GmbH, Ratingen abgeholt und gemäß DIN 66399 datenschutzgerecht entsorgt (gegen Quittung).
- Elektronische und optische Datenträger werden in abgeschlossenen Alu-Tonnen in der IT-Abteilung in einem verschlossen Raum gesammelt und von der Rhenus (Rhenus Data Office GmbH) vor Ort geschreddert.
- Magnetische Datenträger, wie Festplatten und LTO-Bänder, werden inventarisiert und der „Lebenszyklus“ wird dokumentiert.

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

RZ-1
- Active Directory mit Zugangsprotokoll
- Logfiles am Server
- Logfiles in den Firewalls
- Aufzeichnung in den Branchenlösungen von Usern bei der Änderung von Daten
- Datenschutzgerechte Passwortrichtlinien gem. BSI werden vom Domaincontroller vorgegeben

RZ-2
- Benutzername und Kennwort
- Einsatz von Multi-Faktor-Authentifizierung im mobilen Arbeiten
- automatische Sperrung nach 5 Minuten Inaktivität (Pausenschaltung)
- Sperrung des Accounts bei wiederholter Falschanmeldung datenschutzgerechte Passwortrichtlinien gemäß BSI vom Domaincontroller vorgegeben oder vom Mitarbeiter bei der Erstanmeldung selbst generiert
- Active Directory mit Zugangsprotokoll
- Server mit zusätzlichen Administratorpasswörtern
- geschützte WLAN-Netzwerke / für Gäste separates WLAN und Speicherung in verschlüsselten Password-Depots
- Hardware in nicht öffentlichen Bereichen dokumentierte Prozesse bei der Benutzerverwaltung(DIN ISO 27001 und BaFin geprüft)
- Logfiles am Server
- Logfiles in den Firewalls
- Aufzeichnung in den Branchenlösungen von Usern bei der Änderung von Daten

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

RZ-1
- Einsatz von gemanagten Firewall-Systemen
- Virenscanner mit automatischem Update und automatischer Verteilung an die Clients
- Server für Zugriffe von außen stehen in einer DMZ
- 2-Faktor-Authentifizierung im Produkt od | care

RZ-2
- G-Data-Virenscanner mit automatischem Update und automatischer Verteilung an die Clients
- Home-Office-Arbeitsplätze via VPN-Anbindung und Citrix Netscaler Terminal-Server
- Patchmanagement der eingesetzten Software, Treiber und OS über Matrix42
- administrierte Firewalls (Cisco-Appliance aus Enterprise-Bereich)
- Server für externe Zugriffe in einer DMZ

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten, personenbezogenen Daten Zugang haben (Zugriffskontrolle)

RZ-1
- durch differenzierte Berechtigungen gesteuert durch die Anmeldung
- extra Administrationspasswörter für die Server
- nur in ein Projekt involvierte Personen haben auch Zugriff darauf
- auf dem Domaincontroller werden „Rollen angelegt“

RZ-2
- Nur die jeweiligen Programmierer bzw. Systembetreuer haben Zugriff auf ihr System.
- Differenzierte Berechtigungen werden durch die Anmeldung gesteuert.
- Zusätzliche Administratorpasswörter für die Server sind nur den entsprechen-den IT-Mitarbeitern bekannt und werden zusätzlich in einem verschlossenen Umschlag an einem separaten Ort sicher aufbewahrt.
- Zusatzvereinbarung für Systemadministratoren
- Rollenkonzept auf dem Domaincontroller

Integrität (Art. 32 Abs. 1b DSGVO)

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)

RZ-1
- im Bereich der Fernwartung kann es vorkommen, dass Daten des Auftraggebers zu Wartungszwecken zur odITS übertragen werden, sobald jedoch der Fehler behoben ist, werden die Daten zurück zum Auftraggeber transferiert und bei der S1 gelöscht, für die Übertragungen werden gesicherte Verbindungen genutzt
- die Übertragungen werden mit der Standardsoftware TeamViewer und einer telefonisch übermittelten Sitzungsnummer durchgeführt
- der Auftraggeber kann die Wartungsarbeiten mitverfolgen
- im Bereich eva/3 Cloud überträgt der Kunde seine zu synchronisierenden Daten auf einen Server der odITS
- im Bereich Server-Hosting liegt die komplette Datenbank eines eva/3 Kunden auf einem Server der odITS, der Kunde arbeitet online mit einer 2048bit SSL verschlüsselten Remote Desktop Verbindung
- es erfolgt in allen Fällen keinerlei Datenweitergabe an Dritte

RZ-2
- Bei den Verbindungen werden VPN-Tunnelverbindungen genutzt.
- Die Übertragung zu den Rechnungsprüfstellen der Kostenträger erfolgt mit Hilfe des Programms dacota und zertifizierter Schlüssel vom ITSG Trust Center (es wird ein asymmetrisches Kryptosystem mit Public-Private-Key benutzt).
- Der Zugriff auf das Online Kundencenter ist nur nach dokumentierter Authentifizierung möglich.
- Es erfolgt keinerlei Datenweitergabe an Dritte
- durch Authentifizierung von Auftraggebern an die Daten übermittelt werden
- die Systeme werden von der IT-Abteilung der opta data Finance GmbH gehostet bzw. gewartet

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)

RZ-1
- durch Protokolle am Domain-Controller
- durch Server Protokolle
- Änderungen im Programmcode werden protokolliert mit CVS, Ticketsystem

RZ-2
- Protokolle am Domain-Controller
- Server Protokolle
- Protokollierung der Benutzerkennung im selbst erstellten Programmpaket eva/3 RZ bei jeder Datenveränderung.
- Änderungen im Programmcode werden protokolliert mit Jira, Ticketsystem

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle)

RZ-1
- Für Online-Portale werden nur https Verbindungen genutzt
- bei direkten Verbindungen werden VPN–Tunnelverbindungen genutzt
- die Daten werden 256Bit SSL verschlüsselt
- es wird ein asymmetrisches Kryptosystem mit public-private-Key benutzt
- Schlüsselzertifikat mit 2048 Bit Key

RZ-2
- festgelegte Transportwege beim Versand von Daten in Papierform
- Zugriff auf das Online Kundencenter nur über https-Protokoll
- Scannen der ein- und ausgehenden E-Mails vom Virenscanner
- E-Mail-TLS-Verschlüsselung
- Für Online-Portale werden nur https Verbindungen genutzt
- bei direkten Verbindungen werden VPN-Tunnelverbindungen genutzt
- die Daten werden 256 Bit SSL verschlüsselt
- es wird ein asymmetrisches Kryptosystem mit public-privat-Key benutzt
- Schlüsselzertifikat mit 2048 Bit Key

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

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

RZ-1
- alle Server sind mit Raid-Systemen ausgestattet, die die Daten permanent spiegeln
- es gibt automatisierte Backupverfahren mit Protokollen
- alle Server sind an USVs angeschlossen
- die Serverräume sind mit Brand- und Löschanlage, Alarmanlage und Klimaanlage ausgestattet
- es gibt Reserveserver für den Fall eines totalen Ausfalls der Server-Hardware
- die LTO-Bänder werden in einem feuersicheren Tresor in einem anderen Standort aufbewahrt
- es kommt ein Virenscanner mit automatischem Update und automatischer Verteilung an die Server zum Einsatz
- Hardwarefirewalls kontrollieren den Internetverkehr

RZ-2
- Betreib von redundanten Rechenzentren
- Bearbeitung der Störung im Rahmen einer definierten Wiederherstellungsstrategie
- Verfügung von Reserve-Server bei einem Ausfall
- Aufbewahrung der LTO-Bänder in feuersicherem Tresor (DIS120) in anderem Brandabschnitt
- IT-Notfallpläne

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)

RZ-1
- Raid-Systeme melden Plattenausfälle in den Servern
- Klimaanlagen in Serverräumen sind redundant ausgelegt
- Meldung von verschiedenen Systemfehlern (Plattenausfall, CPU-Ausfall, etc.) durch ein Monitoring-System.

RZ-2
- Meldung von verschiedenen Systemfehlern (Plattenausfall, CPU-Ausfall, etc.) durch ein Monitoring-System.
- Meldung von Störungen durch Löschanlagen und Sauerstoffreduzierung
- Umweltüberwachung in den Serverräumen
- Serverräume mit Brand- und Rauchmelder, Alarmanlage, Klimaanlage und Videoüberwachung
- IT-Infrastruktur mit Rufbereitschaft, auch außerhalb der Geschäftszeiten (24 Stunden, 7 Tage in der Woche besetzt)

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

- Vermeidung von Datenhaltung auf lokalen Endgeräten
- Patchmanagement nach DIN ISO 27001

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

RZ-1
- durch Verträge gem. Artt. 28 und 29 DSGVO
- dokumentierte Prozessabläufe
- Schulungen und Sensibilisierungsmaßnahmen

RZ-2
- den Softwareverträgen beiliegende Verträge zur Auftragsverarbeitung und Regelung der Kompetenzen und Pflichten zwischen Auftraggebern und der opta data Finance GmbH
- dokumentierte Prozessabläufe
- interne Schulungen und Weiterbildungen
- Monitoring der gehosteten Systeme
- Verträge gem. Art. 28 und 29 DSGVO
- Verträge zur Teilnahme am HMP-System

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

RZ-1
- alle Server sind an USVs angeschlossen, Netzersatzanlage bei Stromausfall
- Serverräume mit Brand- und Löschanlage, Alarmanlage und Klimaanlage
- der Serverraum ist feuergeschützt durch Feuerschutztür und Stahlwände gem. Brandschutzklasse S30
- IT-Notfallpläne

RZ-2

- automatisiertes Backupverfahren mit Protokollen
- hochverfügbares Storagecluster
- vorhandene redundante Serverräume
- Ausstattung aller Rechenzentren mit Raid-Systemen die Daten permanent spiegeln
- Anschluss aller Server an ausreichend dimensionierte USVs
- Netzersatzanlage zur Überbrückung länger anhaltender Stromausfälle
- Schutz des Serverraums vor Feuer durch Feuerschutztür und Stahlwände
- gemäß Brandschutzklasse S30

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)

- durch interne Mandantenfähigkeit und Authentifizierung der Auftraggeber bzw. der Kostenträger
- verschiedene Systeme sind auch auf unterschiedlichen Servern installiert
- nur die jeweiligen Programmierer bzw. Systembetreuer haben Zugriff auf „ihr" System

Verfahren zur regelmäßigen Überprüfung und Bewertung der technischen und organisatorischen Maßnahmen im Datenschutz gem. Art. 32 Abs. 1d und Art. 25 Abs. 1 DSGVO

Datenschutzmanagement

Es ist zu gewährleisten, dass Verantwortlichkeiten festgelegt werden und die technischen und organisatorischen Maßnahmen regelmäßig überprüft und evaluiert werden

- eine Datenschutzleitlinie ist vorhanden
- Schulung der Mitarbeiter durch den Datenschutzbeauftragten
- interne Audits werden durch den Datenschutzbeauftragten und die Revision durchgeführt
- DIN/ISO 27001 Audits werden durch den TÜV durchgeführt

Incident-Response-Management

- Es bestehen Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder bei geänderten Voraussetzungen erweitert bzw. ergänzt werden
- Notfallpläne
- Datenschutzfolgeabschätzungen gem. Art. 35 DSGVO werden für Prozesse bei denen besondere und sensible Daten verarbeitet werden durchgeführt.

Essen, 25.06.2024 

Ort, Datum — Joachim Kramer
(betrieblicher Datenschutzbeauftragter)

Essen, 25.06.2024 

Ort, Datum — Tobias Windhaus
(Informationssicherheitsbeauftragter)