egeko
einfach effizient

Anlage B zum Rahmenvertrag egeko

Auftragsverarbeitungsvereinbarung bei Nutzung von Softwareprodukten der opta data Finance GmbH (im Folgenden Auftragnehmer)

Diese Vereinbarung regelt die Maßnahmen zum Schutz von personenbezogenen Daten gem. Art. 4 Nr. 1 EU-DSGVO, Gesund-heitsdaten gem. Art. 4 Nr. 15 EU-DSGVO und Sozialdaten im Sinne des § 67 Abs. 2 SGB X bei der Datenverarbeitung im Auftrag unter Berücksichtigung der Art. 28, 29 EU-DSGVO und der § 80 SGB X sowie § 29 KDG, § 29 KDR-OG und §30 DSG-EKD.

1. Gegenstand und Dauer des Auftrags

1.1 **Gegenstand**
Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen mit dem Kunden (im Folgenden Auftraggeber) geschlossenen Softwarevertrag nebst seiner einbezogenen Anlagen, auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung").

1.2 **Dauer**
Die Dauer (Laufzeit) dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung und ist an diese gekoppelt.

2. Konkretisierung des Auftragsinhalts

2.1 **Art und Zweck der vorgesehenen Verarbeitung von Daten**

2.1.1 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 1 zu dieser Auftragsverarbeitung und basiert auf den in der Leistungsvereinbarung gewählten Produkten.

2.1.2 Der Auftragsinhalt ist nicht abschließend. Je nach Wahl von Zusatzdienstleistungen durch den Auftraggeber beim Auftragnehmer kann der Auftragsinhalt über die unter Ziffer 2 geregelten Inhalte hinausgehen. In diesem Fall ergibt sich die Konkretisierung aus der Leistungsvereinbarung.

2.1.3 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.

2.2 **Art der Daten**
Die personenbezogenen Datenarten/-kategorien ergeben sich aus der Anlage 1 dieser AV-Vereinbarung.

2.3 **Kategorien betroffener Personen**
Die Kategorien der durch die Verarbeitung betroffenen Personen ergeben sich aus der Anlage 1 dieser AV-Vereinbarung.

3. Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 S. 2 lit. c), Art. 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen.

3.3 Eine Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 EU-DSGVO ist Bestandteil dieses Auftrags und liegt dieser Vereinbarung als Anlage 2 anbei. 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. Berechtigung, Einschränkung und Löschung von Daten

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

4.2 Soweit im Leistungsumfang definiert, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

5.1 Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung, soweit nach EU-DSGVO bzw. BDSG erforderlich, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-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 Website des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-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 EU-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.
- 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

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post- /Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsunterlagen 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 Vereinbarung sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 EU-DSGVO:

Der Auftraggeber stimmt den in der Anlage 1 aufgeführten Unterauftragnehmern zu.

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

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit, mindestens 14 Tage, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform einen begründeten Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

Im Falle eines Einspruchs finden die Parteien eine einvernehmliche Lösung.

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden, sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen gem. Art. 44 ff. EU-DSGVO sicher. Gleiches gilt, wenn der Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden soll.

6.5 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.

6.6 Dem Einsatz von Mitarbeitern des Auftragnehmers in Heimarbeit oder im mobilen Arbeiten stimmt der Auftraggeber zu.

7. Kontrollrechte und Pflichten des Auftraggebers

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

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-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.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz oder ISO 27001).

7.4 Für die Ermöglichung von Kontrollen, die über ein übliches Maß von einmal jährlich hinaus gehen, kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Dieser darf die tatsächlich entstanden Kosten nicht überschreiten.

7.5 Der Auftraggeber hat seinen Pflichten gegenüber dem Betroffenen gemäß Art. 13 EU-DSGVO nachzukommen und dem Betroffenen mitzuteilen, dass der Auftragnehmer und der einbezogene Unterauftragnehmer die Verarbeitung seiner personenbezogenen Daten involviert sind. Insofern verpflichtet sich der Auftraggeber zur Einhaltung und Umsetzung seiner Pflichten nach der EU-DSGVO.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der EU-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 Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Behörde

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

9. Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Schriftform.

9.2 Der Auftraggeber hat den Auftragnehmer 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

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ausgenommen von dieser Regel sind Daten, die der Auftragnehmer zur Wahrung der gesetzlichen Aufbewahrungsfristen nicht löschen darf.

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

11. Änderungs-Klausel

Der Auftragnehmer ist zu Änderungen dieser AV-Vereinbarung berechtigt. Der Auftragnehmer wird diese Änderungen nur aus triftigen Gründen, insbesondere aufgrund neuer technischer Entwicklungen, Änderungen der Rechtsprechung oder sonstigen gleichwertigen Gründen unter Berücksichtigung des vertraglichen Gleichgewichts durchführen. Die geänderten AV-Vereinbarungen werden dem Auftraggeber schriftlich, über das Online Kundencenter oder per E-Mail zur Verfügung gestellt. Sie werden entweder mit Bestätigung des Auftraggebers im Online Kundencenter oder im Falle schriftlicher oder elektronischer Zusendung wirksam, wenn dem Auftragnehmer nicht innerhalb von zwei Wochen ab Zustellung ein schriftlicher Widerspruch des Auftraggebers eingeht.

12. Schlussbestimmungen

Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den einschlägigen datenschutzrechtlichen Vorgaben genügt.

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.

Anlagen

- Anlage 1: Konkretisierung des Auftragsinhalts
- Anlage 2: Technische und organisatorische Maßnahmen

(Ende der Vereinbarung zur Auftragsverarbeitung)

(Die Vereinbarung ist dem Auftraggeber in Textform übermittelt worden und ohne Unterschrift gültig)

Anlage B zum Rahmenvertrag egeko

Auftragsverarbeitungsvereinbarung Produkte

Inhaltliche Übersicht zu den Auftragsverarbeitungsvereinbarungen der egeko Produkte:

- egeko Care
- egeko connect
- egeko eID
- egeko eKV
- egeko eLNW Care
- egeko Entlassungsmanagement HiMi/HKP
- egeko Hilfsmittelpool
- egeko order
- egeko Versichertencheck
- egeko OCR

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko Care“

Produkt	**egeko Care**
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Im Rahmen des elektronischen Genehmigungsverfahrens kümmert egeko sich um den digitalen Austausch der Genehmigungsanfragen der jeweiligen Leistungserbringer mit den Krankenkassen. Dabei entlastet das elektronische Genehmigungsverfahren nicht nur den Posteingangsprozess; es bietet auch die Grundlage für weitere Effizienzsteigerungen durch automatisierte Bearbeitungsoptionen. Der an sich komplexe Prozess wird damit nicht nur vereinfacht und beschleunigt, er wird auch deutlich transparenter für alle Beteiligten.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO)
Unterauftragnehmer	**Beschreibung**
	Microsoft, Serverstandort Deutschland (E-Mail Kommunikation über Exchange Online, Fernwartung über MS Teams)
	Firmen der “opta data Unternehmensgruppe” (https://www.optadata-gruppe.de/unternehmen/unternehmen-der-gruppe)
	Saldaris GmbH, Leimkugelstraße 13, 45141 Essen (Inkasso)
	opta data dialog GmbH, Essen (Telefonischer Inboundservice, Belegerfassung)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko connect“

Produkt	egeko connect (HiMi)
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Connect ermöglicht es Nutzern von Branchensoftware, ihre Rechnungsdaten elektronisch zu erstellen und diese elektronisch an ein Abrechnungshaus zu liefern.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO) • Betreuer bzw. Erziehungsberechtigte
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice, Belegerfassung)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko eID“

Produkt	egeko eID
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Mit Hilfe der eID können Teilnehmer sich mithilfe ihrer persönlichen PIN eindeutig identifizieren (gemäß § 21 PAuswG für Diensteanbieter) und beim Leistungserbringer eine Vor-Ort-Auslesefunktion durchführen (gemäß § 21a PAuswG für Vor-Ort-Diensteanbieter). Opta Data ist von der bva zertifiziert und bietet im Rahmen des Angebots als Diensteanbieter die eID-Funktionen als Integration an. [Es sind datenschutzrechtliche Vorschriften einzuhalten (gemäß § 21 Abs. 1 S. 2 PAuswG)].
Art der Daten	**Versicherten/Betroffenen-Daten:** • Familienname • Geburtsname • Vorname • Tag der Geburt • Ort der Geburt • Anschrift • Letzter Tag der Gültigkeitsdauer • Nebenbestimmungen • Abkürzung der Staatsangehörigkeit **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO) • Betreuer bzw. Erziehungsberechtigte
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice, Belegerfassung)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko eKV“

Produkt	egeko eID
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Im Rahmen des elektronischen Genehmigungsverfahrens kümmert egeko eKV sich um den digitalen Austausch der Genehmigungsanfragen der jeweiligen Leistungserbringer mit den Krankenkassen. Dabei entlastet das elektronische Genehmigungsverfahren nicht nur den Posteingangsprozess; es bietet auch die Grundlage für weitere Effizienzsteigerungen durch automatisierte Bearbeitungsoptionen. Der an sich komplexe Prozess wird damit nicht nur vereinfacht und beschleunigt, er wird auch deutlich transparenter für alle Beteiligten. Mit egeko eKV wurde das elektronische Genehmigungsverfahren für die Bereiche Hilfsmittel, häusliche Krankenpflege und Fahrkosten umgesetzt.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO) • Betreuer bzw. Erziehungsberechtigte
Unterauftragnehmer	**Beschreibung**
	Microsoft, Serverstandort Deutschland (E-Mail Kommunikation über Exchange Online; Fernwartung über MS Teams)
	Firmen der “opta data Unternehmensgruppe” (https://www.optadata-gruppe.de/unternehmen/unternehmen-der-gruppe)
	Saldaris GmbH, Leimkugelstraße 13, 45141 Essen (Inkasso)
	opta data dialog GmbH, Essen (Telefonischer Inboundservice, Belegerfassung)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko eLNW Care“

Produkt	egeko eLNW Care
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Der eLNW (elektronischer Leistungsnachweis) ermöglicht es dem Leistungserbringer, seine erbrachten Leistungen vollständig digital zu dokumentieren und diese vom Leistungsempfänger digital bestätigen zu lassen.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO)
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko Entlassungsmanagement HiMi/HKP“

Produkt	**egeko Entlassungsmanagement HiMi/HKP**
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Als Schnittstelle zum Patientenportal erleichtert egeko das Entlassmanagement für Patient:innen, Healthcare-Professionals und Krankenkassen. Neben vielen weiteren Leistungen wird vor allem der Prozess rund um die notwendigen Leistungen beim Übergang von der stationären in die ambulante Versorgung optimiert. Sobald also eine Klinik im Rahmen des Entlassmanagements eine erforderliche Leistung in das System eingibt, werden, basierend auf verschiedene Datenquellen, die für die individuelle Versorgung in Frage kommenden Leistungserbringer angezeigt. Aufgrund dieser Informationen kann der Sozialdienst der Klinik gemeinsam mit den Patient:innen passende Angebote auswählen. Alle notwendigen Prozessschritte werden dabei vollständig digital abgebildet.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO) • Betreuer bzw. Erziehungsberechtigte
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko Hilfsmittelpool

Produkt	**egeko Hilfsmittelpool**
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Der Wiedereinsatz von gebrauchten Hilfsmitteln ist nicht nur aus Gründen der Nachhaltigkeit sinnvoll. Er stellt oftmals auch die wirtschaftlichere Alternative zur Neuversorgung dar und trägt dazu bei, Leistungsausgaben zu senken. Die egeko-Hilfsmittelpoolverwaltung ist vollständig in den Versorgungsprozess integriert und unterstützt sämtliche Teilprozesse im Zusammenhang mit dem Wiedereinsatz von Hilfsmitteln – von der Rückholung, über den Wiedereinsatz bis hin zur Aussonderung. Als exklusives Poolverwaltungssystem der Techniker Krankenkassen wird der egeko-Hilfsmittelpool bereits von mehr als 3.500 Leistungserbringern genutzt.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO)
Unterauftragnehmer	**Beschreibung**
	Microsoft, Serverstandort Deutschland (E-Mail-Kommunikation über Exchange Online)
	Firmen der "opta data Unternehmensgruppe" (https://www.optadata-gruppe.de/unternehmen/unternehmen-der-gruppe)
	Saldaris GmbH, Leimkugelstraße 13, 45141 Essen (Inkasso)
	opta data dialog GmbH, Essen (Telefonischer Inboundservice)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko order

Produkt	egeko order
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Mit egeko Order wird der Bestellvorgang von Hilfsmitteln sicher, durchgängig und digital. Da der digitale Auftragsverarbeitungsprozess auch administrative Funktionen beinhaltet, entfallen umständliche und teilweise doppelte Eingaben von Daten: Bestellbestätigungen, Rechnungen und Lieferscheine werden automatisiert in einem einzigen System erstellt. Alle Artikelstammdaten sind zuverlässig auf dem neuesten korrekten Stand. Mit einem Blick können Ihre Kund:innen beispielsweise Lieferungen einfach verfolgen. egeko Order ist in jede ERP-Software der opta data Gruppe integriert (z.B. eva3, acriba, orthosoft, ipn) und ebenfalls kompatibel mit Lösungen anderer Anbieter.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO) • Betreuer bzw. Erziehungsberechtigte
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko Versichertencheck“

Produkt	**egeko Versichertencheck**
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: Der egeko Versichertencheck ermöglicht es den ERP SE der Leistungserbrunger vor dem Einreichen einer elektronischen Genehmigungsanfrage zunächst den Versicherten- und Zuzahlungsstatus der jeweiligen Patienten über einen sicheren WebService unmittelbar aus der Branchensoftware abzufragen. Dieser Service verbessert die Qualität der eingehenden Daten und erhöht damit die Chance einer automatisierten Bearbeitung.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO)
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice)

Anlage B zum Rahmenvertrag egeko

Anlage 1 - Auftragsverarbeitungsvereinbarung Produkt „egeko OCR“

Produkt	**egeko Versichertencheck**
Konkretisierung des Auftragsinhalts	Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten: odFIN bietet mit diesem Produkt das Auslesen von eingescannten Hilfsmittelverordnungen mittels automatischer Texterkennung und die digitale Übermittlung per Schnittstelle an die Branchensoftware des Kunden an.
Art der Daten	**Versicherten/Betroffenen-Daten:** • Adressdaten • Kontaktdaten, bei Anfragen von Versicherten • Geburtsdatum • Geschlecht • Gesundheitsdaten • Sozialdaten • Versichertendaten • Zuständige Ärzte • ggf. Adress- und Kontaktdaten von Betreuern und Erziehungsberechtigten **Kundendaten:** • Rechnungsdaten • Adressdaten • Zahlungsdaten • Kundenhistorie • Vertragsstammdaten • Kontakt-/Kommunikationsdaten
Kategorien betroffener Personen	• Auftraggeber • Mitarbeiter des Auftraggebers • Versicherte/Betroffene (gesetzlich bzw. privat Versicherte – betroffene Personen im Sinne des Art. 1. EU-DSGVO) • Betreuer bzw. Erziehungsberechtigte
Unterauftragnehmer	**Beschreibung**
	opta data dialog GmbH, Essen (Telefonischer Inboundservice)

egeko
einfach effizient

Anlage B zum Rahmenvertrag egeko

Anlage 2 - Anlage zur Auftragsverarbeitungsvereinbarung

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

Vorwort

Die familiengeführte opta data Gruppe entwickelt seit über 50 Jahren passgenaue Services und digitale Lösungen für den betrieblichen Alltag in verschiedensten Bereichen des Gesundheitswesens – mit dem Ziel, die nahezu 60.000 Kund:innen bestmöglich zu unterstützen. Über 2.500 engagierte Mitarbeiter:innen bieten darüber hinaus bankenunabhängige Finanzierungen, digitale Kommunikationsprodukte oder gezieltes Telefonmarketing.

Als Innovationsführer gestalten wir die Digitalisierung des Gesundheitswesens aktiv mit und sind Marktführer auf dem Gebiet der Telematikinfrastruktur.

Wir legen großen Wert auf die Zufriedenheit unserer Kund:innen und die Gesundheit unserer Kolleg:innen. Ein Einsatz, für den wir mehrfach ausgezeichnet wurden: mit den Siegeln „Top Job", „Deutschlands Kundenchampions" und dem „Corporate Health Award" für unser Engagement im betrieblichen Gesundheitsmanagement.

Diese Auflistung der bei der opta data Finance GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) orientiert sich an den Vorgaben des § 64 BDSG, der für nicht öffentliche Stellen keine Gültigkeit hat, gleichzeitig aber eine strukturierte Dokumentation der TOMs ermöglicht, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im neuen Bundesdatenschutzgesetz (BDSG) dazu Vorgaben für nicht öffentliche Stellen gibt. Diese Angaben dokumentieren auch die Forderungen des § 26 KDG, § 26 KDR-OG, § 6 KDO und des Art. 32 der DSGVO. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihre Prüfund Dokumentationspflicht bei Auftragsverarbeitung gem. Artt. 28, 29 DSGVO, § 29 KDG, § 29 KDR-OG, § 8 KDO und § 80 SGB X zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Art. 28, 29 DSGVO bzw. §29 KDG, § 29 KDR-OG oder § 8 KDO -konformen Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhandene Sicherheitsniveau nicht verringert wird.

Ergänzend sei noch erwähnt, dass es bei der opta data Finance GmbH IT-Notfallpläne, Datensicherungs-, Berechtigungs und Löschkonzepte sowie dokumentierte Prozessabläufe gibt.

Konkretisierung des Auftragsinhalts

1. Verantwortliche
opta data Finance GmbH
Berthold-Beitz-Boulevard 461
45141 Essen

Telefon: 0201 3196-0
E-Mail: service@optadata-gruppe.de

2. Ansprechpartner mit Telefon, Fax und E-Mail
Kundenmanagement
E-Mail: service@optadata-gruppe.de

Internes Datenschutzmanagement
E-Mail: datenschutzmanagement@optadata-gruppe.de

Informationssicherheits-Beauftragter (ISB)
E-Mail: informationssicherheitsmanagement@optadata-gruppe.de

3. Name und Kontaktdaten des Datenschutzbeauftragten
Datenschutz Kramer & Kramer GmbH
Büro für Datenschutz und Datensicherheit
Elsternweg 24
42555 Velbert

Telefon: 02052 92897-66
E-Mail: j.kramer@datenschutz-kramer.de

4. Datenschutzbeauftragter

4.1 Bestellung

- externer Datenschutzbeauftragter gem. Art. 37 DSGVO
- Die schriftliche Bestellung vom 05.09.2009 liegt vor.
- Ehemals war Herr Günter Wolfgang Kramer, staatl. gepr. Betriebswirt
- EDV, externer Datenschutzbeauftragter (01.09.1987 – 04.09.2009).

4.2 Qualifikation:

- Datenschutz-Auditor (TÜV), Zertifizierungsstelle für Personal TARZERT
- der TÜV Akademie Rheinland, Nr. 19553
- über 20 Jahre Erfahrung im IT-Bereich
- regelmäßige Fortbildungen
- Mitglied im Erfa-Kreis für Datenschutzbeauftragte der Region MEO
- GDD Mitglied
- Firma Datenschutz Kramer & Kramer GmbH mit über 30 Jahren
- Erfahrung im Datenschutz

5. Mitarbeiter der opta data Finance GmbH

- Alle Mitarbeiter werden schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB und der Vertraulichkeit nach DSGVO, BDSG und SGB verpflichtet. Die Verpflichtung erfolgt auf einem seperaten Formular.
- Die der Verpflichtung zugrunde liegenden Gesetzestexte werden allen Mitarbeitern gegen Unterschrift ausgehändigt.
- Die Verpflichtung wird bei Einstellung durch das Personalbüro der opta data Finance GmbH vorgenommen.
- Von allen Mitarbeitern werden in sensiblen Bereichen werden polizeiliche Führungszeugnisse eingeholt.
- Alle Mitarbeiter werden regelmäßig durch den DSB zum Thema „Datenschutz und Datensicherheit" geschult.
- Eine Betriebsvereinbarung über die private Nutzung von E-Mail, Internet, Telefon und den Umgang mit Hard- und Software wird ausgehändigt.
- Darüber hinaus existieren Richtlinien zur Informationssicherheit und dem Datenschutz, die allen Mitarbeitern zentral zur Verfügung gestellt werden.

6. Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO

- Das „Verzeichnis der Verarbeitungstätigkeiten" liegt vor und ist Bestandteil eines Integrierten Managementsystems, in dem auch das Qualitäts-, Arbeitsschutz-, Risiko- und Notfallmanagement abgebildet werden.

Technische und organisatorische Maßnahmen:

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

- 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 authorisieren den Zutritt.
- Die Zentrale im Berthold-Beitz-Boulevard 461 ist rund um die Uhr, an 7 Tagen in der Woche besetzt.
- Der Wachdienst fährt außerhalb der Arbeitszeiten alle Standorte der Unternehmensgruppe in Essen regelmäßig an.
- Die Serverräume sind mit seperaten Sicherheitsschlössern bzw. Zahlencode-Schlössern ausgestattet.
- Es kann nachvollzogen werden, welche Tür wann und von wem geöffnet wurde (Logfiles in den Türzutrittssystemen).

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

- 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 verschlossenen 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.

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

- 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

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

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

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

- 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 entsprechenden IT-Mitarbeitern bekannt und werden zusätzlich in einem verschlossenen Umschlag an einem separaten Ort sicher aufbewahrt.
- Zusatzvereinbarung für Systemadministratoren
- Rollenkonzept auf dem Domaincontroller

6. 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):

- 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

7. 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) durch:

- 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

8. **Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle) durch:**
   - festgelegte Transportwege beim Versand von Daten in Papierform
   - Zugriff auf das Online Kundencenter nur über https-Protokoll
   - Scannen der ein- und ausgehende E-Mails vom Virenscanner
   - E-Mail -TLS-Verschlüsselung
   - Für Online-Portale werden nur https Verbindungen genutzt
   - bei direkten Verbindungen werden VPN-Tunnelverbindungengenutzt
   - die Daten werden 256Bit SSL verschlüsselt
   - es wird ein asymmetrisches Kryptosystem mit publicprivate-Key benutzt
   - Schlüsselzertifikat mit 2048 Bit Key

9. **Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit) durch:**
   - Betrieb 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 (DIS 120) in anderem Brandabschnitt
   - IT-Notfallpläne

10. **Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) durch:**
    - 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)

11. **Gewährleistung, dass gespeicherte, personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität) durch:**
    - Vermeidung der Datenhaltung auf lokalen Endgeräten
    - Patchmanagement nach DIN ISO 27001

12. **Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle) durch:**
    - 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

13. **Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle) durch:**
    - 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

14. **Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit) durch:**
    - interne Mandantenfähigkeit
    - Installation verschiedener Systeme auf unterschiedlichen Servern
    - Trennung von Produktiv- und Testsystem

15. **Verfahren zur regelmäßigen Überprüfung und Bewertung der technischen und organisatorischen Maßnahmen im Datenschutzgem. Art. 32 Abs. 1 d) und Art. 25 Abs. 1 DSGVO:**
    - Ein Datenschutzmanagement wurde eingeführt.
    - Das Datenschutzmanagement-Team wird in die Planung neuer oder geänderter Projekte einbezogen und führt in regelmäßigen Abständen interne Audits durch.
    - Verantwortlichkeiten wurden festgelegt und technische und organisatorischen Maßnahmen werden regelmäßig evaluiert und aktualisiert.
    - eine Datenschutzleitlinie ist vorhanden
    - regelmäßige Schulungen der Mitarbeiter durch den Datenschutzbeauftragten
    - interne Audits werden regelmäßig durch das Datenschutzmanagement und das Qualitätsmanagement durchgeführt
    - Revision mit internen Audits

16. **Incident-Response-Management:**
    - Es gibt Richtlinien, Handlungsanweisungen und Prozesse, die beigeänderten Voraussetzungen und bei Gesetzesänderungen angepasst werden. Ferner werden Prozesse immer wieder auf Funktionalität überprüft und ggf. angepasst oder erweitert
    - Grafisch visualisierte Handlungsanweisungen für verschiedene Datenschutzprozesse wie z. B. Einbindung des DSB, Meldewege, Betroffenenrechte etc.
    - Datenschutzfolgeabschätzungen gem Art. 35 DSGVO werden für Prozesse bei denen besondere und sensible Daten verarbeitet werden durchgeführt.