dekodi
umwandeln » beschleunigen » gewinnen

Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO

Stand 06.12.2023

dekodi - Deutscher Konverterdienst GmbH
Benno-Strauß-Straße 7B 90763 Fürth
Geschäftsführer: Stefan Kaumeier
Telefon 0911 / 310 429 10· Telefax 0911 / 310 429 99
info@dekodi.de · www.dekodi.de

Vereinbarung gemäß Art. 28 DS-GVO

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt –

und dem/der

dekodi – Deutscher Konverterdienst GmbH
Benno-Strauß-Str. 7/B
90763 Fürth

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

Dieser Ergänzungsvertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den zwischen Auftraggeber und Auftragnehmer geschlossenen Vertragsverhältnissen ergeben, auf die hier verwiesen wird. Er findet Anwendung auf alle Tätigkeiten, die mit diesen Vertragsverhältnissen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieses Ergänzungsvertrages richtet sich nach der Laufzeit der geschlossenen Vertragsverhältnisse.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in den zwischen Auftraggeber und Auftragnehmer geschlossenen Vertragsverhältnissen beschrieben, auf die hier verwiesen wird.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Eine Verlagerung von Daten oder Datenverarbeitungsaufträgen wird derzeit nicht durchgeführt.

(2) Art der Daten

- Personenstammdaten
- Alle Daten, die vom Auftraggeber bereitgestellt werden (vorbehaltlich einer konkreten Verarbeitung in den vereinbarten Schnittstellen-Prozessen)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten

(3) Kategorien betroffener Personen

- Kunden/Mandanten
- Interessenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

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

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

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

4. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, 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 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

- Als Datenschutzbeauftragte(r) ist beim Auftragnehmer

  Herr Reinhold Csakli
  Munker Privacy Consulting GmbH,
  Zugspitzstraße 3a
  82399 Raisting
  Telefon: 08807-244 47-0
  Email: dsb@munker.info

  bestellt.

- Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) 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.

f) 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.

g) 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer bindet Unterauftragnehmer unter folgenden Voraussetzungen ein.
Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mindesten 6 Wochen vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Der Auftragnehmer behält sich für den Fall eines Widerspruchs des Auftraggebers vor, andere Verträge zwischen Auftraggeber und Auftragnehmer, die diesen AV-Vertrag bedingen, zu beenden.

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

Die derzeit eingesetzten Unterauftragnehmer sind der Anlage 2 zu entnehmen.

7. Kontrollrechte des Auftraggebers

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

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

3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

(4) Die Ausübung der Kontrollen durch den Auftraggeber ist grundsätzlich kostenlos.
Der Auftragnehmer behält sich jedoch – insbesondere unter dem Gesichtspunkt der Verhältnismäßigkeit der Kontrollen – vor, einen Vergütungsanspruch geltend zu machen.

8. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(2) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

a. besondere Arten bzw. besondere Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO oder
b. personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
c. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
d. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

(3) Soweit die getroffenen Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen. 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.

(5) Soweit eine betroffene Person sich bezüglich Ihrer Betroffenenrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(6) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Personen nachkommen kann.

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber behält sich hinsichtlich der Auftragsverarbeitung ein umfassendes Weisungsrecht vor. Alle Aufträge, Teilaufträge oder Weisungen werden dokumentiert erteilt. In Eilfällen können Weisungen mündlich gegeben werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen. Dieses Recht wird durch den Geschäftsführer bzw. durch ihn ausdrücklich autorisierte Personen wahrgenommen.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich entsprechend der vertraglichen Vereinbarung nach diesen Weisungen es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

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

(4) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10. Löschung und Rückgabe von personenbezogenen Daten

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

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

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

Datum/Unterschrift Auftraggeber

ppa. Christa Kaumeier

Datum/Unterschrift Auftragnehmer

Anlage 1

Technisch-organisatorische Maßnahmen beim Auftragsverarbeiter

Dekodi – Deutscher Konverterdienst GmbH
Benno-Strauß-Straße 7 A/B
90763 Fürth

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Schlüsselregelung (Schlüsselausgabe etc.)
- Manuelles Schließsystem
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Gehäuseverriegelung
- Erstellen von Benutzerprofilen
- Schlüsselregelung (Schlüsselausgabe etc.)
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal
- Verschlüsselung von mobilen Datenträgern
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Einsatz von zentraler Smartphone-Administrations-Software
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Datenträgern in Laptops / Notebooks

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministratoren
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern.
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Protokollierung der Vernichtung

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)

Pseudonymisierung

Maßnahmen, die gewährleisten, dass Datenschutzgrundsätze, wie etwa Datenminimierung, wirksam umgesetzt und die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen dieser Verordnung zu genügen.

- Die Pseudonymisierung ist im Verarbeitungsprozess so früh wie möglich durchzuführen
- Pseudonymisierung wird zum Schutz der Vertraulichkeit wann immer möglich praktiziert

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Das Mitbringen privater Datenträger ist untersagt

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Serverräume liegen nicht unter sanitären Anlagen
- Feuerlöschgeräte in Serverräumen
- In Hochwassergebieten: Serverräume über der Wassergrenze

Rasche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans

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

Datenschutz-Management

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschützers gerecht wird.

- Regelmäßige Schulung der MitarbeiterInnen zum Datenschutz
- Die Aufbewahrung der elektronischen Protokolle ist geregelt
- Es gibt Regelungen über die Sicherung des Datenbestands
- Schriftliche Bestellung eines Datenschutzbeauftragten
- Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden
- Ein Datenschutzkonzept ist vorhanden
- Protokoll- und Log-Dateien werden regelmäßig ausgewertet
- Datenschutz- und Datensicherungsmaßnahmen werden gelegentlich unvermutet kontrolliert

Incident-Response-Management

Maßnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an den Auftraggeber erfolgt.

- Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne
- Es gibt ein Konzept zur Meldung von Datenpannen an den Auftraggeber

Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass den Vorgaben Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge getan wird.

- Alle Einstellungen auf der Webseite www.dekodi.de sind so gesetzt, dass keine automatische Zustimmung zur Übermittlung von (personenbezogenen) Daten erfolgt.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftliche Weisung an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen
- Verpflichtung der Mitarbeiter zur Vertraulichkeit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

ppa. Christa Kaumeier

Datum/Unterschrift Verantwortlicher für die Erstellung

Anlage 2

Unterauftragsnehmer

Dekodi – Deutscher Konverterdienst GmbH
Benno-Strauß-Straße 7 A/B
90763 Fürth

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Unterauftragnehmer im Sinne des Art. 28 DS-GVO in Anspruch zu nehmen
Die jeweils aktuell eingesetzten Unterauftragnehmer sind in der nachfolgenden Übersicht aufgelistet:

Unterauftragnehmer	Betroffene Dienstleistung	Zweck	Rechtsgrundlage
Noris Network AG Thomas-Mann-Straße 16-20 90471 Nürnberg	Rechen-zentrumsleistungen	Bereitstellung von Cloudbasierter IT-Infrastruktur, ein-schließlich Service und Support und Fehleranalyse.	Art. 28 DSGVO
Mittwald CM Service GmbH & Co. KG Königsberger Straße 6 32339 Espelkamp	Rechen-zentrumsleistungen Webhosting	Bereitstellung von Servern und Appli-kationen für Web-hosting und Ab-rechnungsdienste, einschließlich Ser-vice, Support und Fehleranalyse	Art. 28 DSGVO
Microsoft Ireland Operation Ltd Atrium Building Block B Carmenhall Road Sandford Industrial Estate Dublin 18 Ireland	Rechen-zentrumsleistungen	Bereitstellung von Cloudbasierter IT-Infrastruktur, ein-schließlich Service und Support und Fehleranalyse.	Art. 28 DSGVO, sowie Standard Contrac-tual Clauses (SCC) zwischen Microsoft Irland und Microsoft USA.

Anlage 3

Verpflichtungserklärung eines Fremdunternehmens zur Verschwiegenheit nach § 203 Strafgesetzbuch

der Firma: **dekodi – Deutscher Konverterdienst GmbH, Benno-Strauß-Str. 7/B, 90763 Fürth**

– nachstehend Auftragnehmer genannt -

gegenüber den beim Auftraggeber tätigen Berufsgeheimnisträgern

(1) Der Auftragnehmer wirkt als Dienstleister an den Tätigkeiten der Berufsgeheimnisträger mit, die einer beruflichen Verschwiegenheitsverpflichtung unterliegen. Der Auftragnehmer wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) und den sonst anwendbaren rechtlichen Vorschriften fremde Geheimnisse, die ihm zugänglich gemacht werden.

(2) Der Auftragnehmer verpflichtet sich, sich nur insoweit Kenntnis von fremden Geheimnissen im Sinne der vorstehenden Ziffer 1 zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.

(3) Beim Einsatz von Dritten verpflichtet sich der Auftragnehmer, diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Zusatzvereinbarung erlangen könnten.

(4) Die Pflicht zur Verschwiegenheit besteht auch nach Beendigung des Auftragsverhältnisses zeitlich unbegrenzt fort.

(5) Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Auftragnehmer auf Grund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragnehmer den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

(6) Der Auftragnehmer verpflichtet sich sicherzustellen, dass die Arbeiten nur durch die auf besondere Verschwiegenheit verpflichteten Mitarbeiter durchgeführt werden.

ppa. Christa Kaumeier

Unterschrift Auftragnehmer

Änderungsindex

Datum	Beschreibung
26.04.2018	Erstausgabe
12.10.2020	Anpassungen an aktuelle Rechtsprechung in Abschnitt 6
23.01.2023	Anlage 1 (technisch organisatorische Maßnahmen), bisherige Anlage 2 (technisch organisatorische Maßnahmen beim Auftragsverarbeiter zu Anlage 1 gemacht), neue Anlage2 / Unterauftragnehmer ergänzt
29.03.2023	Anpassung Beauftragung Unterauftragnehmer (Abschnitt 6 (2)) neu formuliert.
25.04.2023	Kapitel 2 Abs 2.: Punkt 2 „Alle Daten, die (…) bereitgestellt werden (…)“ erfasst. Kapitel 8 und 9 wurden überarbeitet.
09.11.2023	Kapitel 8, Abs. 6.: Verweis auf DS-GVO von Kapitel II auf Kapitel III geändert.
06.12.2023	Kapitel 7, Abs. 4: Vergütungsanspruch für Kontrollen konkretisiert