

Datenschutzrechtliche Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag („Auftragsverarbeitungsvertrag“)

Zwischen dem Verantwortlichen:

Lizenznehmer der KODE GmbH

-nachstehend „Auftraggeber (AG)“ genannt-

und dem Auftragsverarbeiter:

KODE® GmbH

Arzbergerstraße 10

D-82211 Herrsching a. Ammersee

vertreten durch Stephan Coester (Geschäftsführer)

-nachstehend „Auftragnehmer (AN)“ genannt-

wird die folgende Vereinbarung zur Datenverarbeitung getroffen:

Präambel

Diese Vereinbarung wird unter Beachtung des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (DSGVO) sowie aller sonstigen einschlägigen datenschutzrechtlichen Vorschriften geschlossen. Für diese Vereinbarung gelten die jeweils in Kraft stehenden Gesetzesvorschriften in ihrer jeweils aktuellen Fassung.

Diese Vereinbarung betrifft die Erhebung, Verarbeitung und Nutzung personenbezogener Daten i. S. d. BDSG und DSGVO durch den Auftragnehmer im Auftrag des Auftraggebers („Auftragsverarbeitung“). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person („Betroffener“). Die Vereinbarung hat die Auftragsverarbeitung von personenbezogenen Daten zum Gegenstand („Auftragsdaten“).

Vor diesem Hintergrund vereinbaren die Parteien Folgendes:

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der wesentliche Gegenstand des Auftrags zum Datenumgang ist die Bereitstellung des cloud-basierten Kode-Verfahrens durch den Auftragnehmer. Dies umfasst die Entwicklung, Implementierung und Bereitstellung des Verfahrens als webbasierte Anwendung in der Cloud. Der Auftragnehmer gewährleistet den reibungslosen Betrieb der Anwendung, einschließlich der kontinuierlichen Wartung, Fehlerbehebung und des technischen Supports. Updates, Anpassungen und die Sicherstellung der Funktionsfähigkeit werden ebenfalls durch den Auftragnehmer übernommen.

Der detaillierte Gegenstand des Auftrages ergibt sich aus dem zugehörigen Dienstleistungsvertrag, auch Hauptvertrag oder Leistungsvereinbarung genannt.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung.

(2) Ort der Verarbeitung

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

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/- Kategorien (Aufzählung/ Beschreibung der Datenkategorien)

- Stammdaten (z. B. Namen, Anschriften, Geburtsdaten),
- Kontaktdaten (z. B. E-Mail-Adressen, Telefonnummern, Messengerdienste),
- Inhaltsdaten (z. B. Texteingaben, Fotografien, Videos, Inhalte von Dokumenten/Dateien),
- Vertragsdaten (z. B. Vertragsgegenstand, Laufzeiten, Kundenkategorie),
- Zahlungsdaten (z. B. Bankverbindungen, Zahlungshistorie, Verwendung sonstiger Zahlungsdienstleister),
- Nutzungsdaten (z. B. Verlauf auf unseren Web-Diensten, Nutzung bestimmter Inhalte, Zugriffszeiten),
- Verbindungsdaten (z. B. Geräte-Informationen, IP-Adressen, URL-Referrer), und
- Standortdaten (z. B. GPS-Daten, IP-Geolokalisierung, Zugriffspunkte).

(4) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden und Interessenten des Auftraggebers
- Beschäftigte des Auftraggebers

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

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

4. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO, sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

(4) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung,

Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- b) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO [Einzelheiten in Anlage 1].
- c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- d) 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.
- e) 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.
- f) 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.

- g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrags.
- h) Der Auftragnehmer wird nach den Weisungen des Auftraggebers angemessene Maßnahmen ergreifen, um weitere unrechtmäßige Kenntnisnahmen durch Dritte auszuschließen und/oder weitere Beeinträchtigungen von den Betroffenen abzuwenden. Bis zu etwaigen Weisungen des Auftraggebers wird der Auftragnehmer alle zur Datensicherung und Schadensminimierung erforderlichen Maßnahmen ergreifen.
- i) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner gesetzlichen Pflichten, insbesondere Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Informationspflichten gegenüber Betroffenen und Aufsichtsbehörden, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Dasselbe gilt auch dann, wenn der Auftraggeber 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 ausgesetzt ist.
- j) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten, die dem Auftraggeber zugehörig sind, bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

6. Unterauftragsverhältnisse

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

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

- a) ☐ Eine Unterbeauftragung ist unzulässig.
- b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
United Internet AG (1und1 IONOS)	Elgendorfer Straße 57 56410 Montabaur Deutschland	Serverhosting, Datenspeicherung, E-Mail Kommunikationsleistungen
Microsoft Ireland Operations Ltd	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Irland	Bereitstellung AZURE Plattform und DevOps; Microsoft 365 (E-Mail, Office-Produkte, Datenspeicherung und -transport)
ISB Information u. Kommunikation GmbH & Co. KG	Lindberghring 6a 33142 Büren Deutschland	Kundenbetreuung, Support, Systembetrieb (Operations)

- c) ☒ Die Auslagerung auf weitere als die unter b) bereits genehmigten Unterauftragnehmer oder / der Wechsel der bestehenden Unterauftragnehmer ist zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mindestens 2 Wochen vorher vorab schriftlich oder in Textform anzeigt und
 - Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

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

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

(5) Eine zusätzliche Auslagerung durch den Unterauftragnehmer auf weitere Unterauftragnehmer:

- ☐ ist nicht gestattet;
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☒ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

Der Auftragsverarbeiter hat sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

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 durch den Auftragnehmer und dessen Unterauftragnehmern am jeweiligen Ort der Verarbeitung der personenbezogenen Daten des Auftraggebers zu überzeugen.

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

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch beispielsweise

- 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).

8. Mitteilung bei Verstößen des Auftragnehmers

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

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

(2) Die Meldung an den Verantwortlichen bei Schutzverletzungen kann über die üblichen (elektronischen, telefonischen) Kommunikationskanäle getätigt werden. Vor dem Hintergrund der Meldepflichten wird der schnellstmögliche Informationsaustausch gewährleistet.

9. Haftung

Zur Haftung gelten die Regelungen des Art. 82 DSGVO.

Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

10. Weisungsbefugnis des Auftraggebers

Die Entscheidungs- bzw. Weisungsbefugnis für die Auftragsverarbeitung hat allein der Auftraggeber. Der Auftragnehmer führt die Auftragsverarbeitung ausschließlich im Rahmen der Vereinbarung und nach schriftlichen Weisungen des Auftraggebers durch, wobei die Weisungen vorrangig gelten, oder wenn eine gesetzliche Verpflichtung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung besteht. Mündliche Weisungen wird der Auftraggeber unverzüglich in Schriftform oder in Textform bestätigen. Der Auftragnehmer ist nicht berechtigt, ohne vorherige Zustimmung in Schrift- oder Textform durch den Auftraggeber Erklärungen gegenüber den Betroffenen abzugeben. Im Falle einer gesetzlichen Verpflichtung teilt der Auftragnehmer dem Auftraggeber diese Verpflichtung vor der Verarbeitung mit.

Der Auftragnehmer darf die Auftragsdaten nicht eigenmächtig, sondern nur nach schriftlicher Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Der Auftragnehmer wird den Auftraggeber über sämtliche Anfragen und Beanstandungen der Betroffenen unverzüglich schriftlich unterrichten sowie den Auftraggeber bei Wahrung der Rechte der Betroffenen unterstützen, wie z. B. durch Benachrichtigung, Auskunftserteilung oder Berichtigung, Sperrung und Löschung von Auftragsdaten.

Die Parteien beachten im Rahmen der Auftragsverarbeitung die einschlägigen datenschutzrechtlichen Vorschriften. Ist der Auftragnehmer der Ansicht, dass eine Vereinbarung oder Weisung gegen datenschutzrechtliche Vorschriften verstößt, wird er den Auftraggeber hierüber unverzüglich schriftlich informieren. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung, solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

11. 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 des Rechts der Union oder des auf den Auftragnehmer anwendbaren Rechts des Mitgliedsstaates 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.

(4) Der Auftraggeber und der Auftragnehmer vereinbaren einen Ausschluss des zivilrechtlichen Zurückbehaltungsrechts nach § 273 BGB zum Ausschluss der Zurückhaltung von verarbeiteten personenbezogenen Daten und Datenträgern im Falle von Vertrags-/Leistungsstörungen.

12. Geheimhaltung

Der Auftragnehmer wird die im Rahmen der Auftragsverarbeitung empfangenen Informationen und Unterlagen, insbesondere die Auftragsdaten, streng geheim halten („Geschäfts- und Betriebsgeheimnisse“). Die Geheimhaltungs-/Verschwiegenheitspflichten gelten auch nach Beendigung dieser Vereinbarung unbefristet fort.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Die Geheimhaltungspflicht gilt nicht oder entfällt, wenn die Informationen und Unterlagen bereits bei Abschluss dieser Vereinbarung der Öffentlichkeit oder dem Auftragnehmer bekannt waren oder nach Abschluss dieser Vereinbarung der Öffentlichkeit bekannt werden, ohne dass den Auftragnehmer hieran ein Verschulden trifft, oder dem Auftragnehmer durch einen Dritten bekannt werden, vorausgesetzt der Dritte verletzt bei Übergabe der Informationen keine eigene Geheimhaltungsverpflichtung. Nachweispflichtig für diese Tatbestände ist der Auftragnehmer.

13. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

(4) Es gilt deutsches Recht.

(Ort, Datum)

(Unterschrift Auftraggeber)

(Ort, Datum)

(Unterschrift Auftragnehmer)

Anlage 1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

Zutrittskontrolle

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

Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Haupttüre der Geschäftsräume mit Knauf auf Außenseite
- Manuelles Schließsystem mit Sicherheitsschlössern am Haupteingang
- Schlüsselregelung / Schlüsselliste
- Sorgfalt bei Auswahl von Mitarbeitenden oder Servicefirmen (z. B. Reinigungsdienst)
- dokumentierte und rollenabhängige Zutrittsberechtigungen
- Besucher dürfen sich grundsätzlich nur in Begleitung von Mitarbeitenden in den Diensträumen aufhalten

Zugangskontrolle

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

Möglichkeiten sind beispielsweise Bootpassword, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarte zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung
- Zuteilung von Benutzerberechtigungen
- Anti-Virus-Software auf Server und PC-Clients
- Trennung von Firmen-Netz und Besucher-WLAN
- dokumentierte Richtlinien zum Datenschutz / Datensicherheit
- Mobile Datenträger sind verschlüsselt
- Laufwerke sind verschlüsselt
- Automatische Sperre von Desktops nach wenigen Minuten Inaktivität
- Clean Desk-Policy (bei Verlassen der Diensträume)

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.

Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Aktenvernichter mit mind. Sicherheitsstufe P-4
- Minimale Anzahl Administrierende
- Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip
- Trennung von Anwendungs- und Administrationszugängen (User-/Admin-Accounts)
- Nutzung kryptografischer Verfahren (z.B. Verschlüsselung)
- Protokollierung von Zugriffsversuchen (sofern Systeme dies zulassen)

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Trennung von Demonstrations-, Entwicklungs-, Test- und Produktivdaten
- Personenbezogene Daten dürfen nicht für Demo- oder Testzwecke verwendet werden
- Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Berechtigungskonzepte, Zweckattribute, strukturierte Dateiablage

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

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Aktuell keine Maßnahmen notwendig/umgesetzt

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

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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do-Prinzips
- Personenbezogene Daten werden nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden
- Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag
- Weitergabe in anonymisierter oder pseudonymisierter Form, sofern möglich
- Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. HTTPS)
- E-Mail-Versand über gesicherte Verbindungen
- Vertrauliche Dateien im E-Mail-Anhang werden mit Sicherheits-Software (z. B. FTAPI) versandt

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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Aktuell keine Maßnahmen notwendig/umgesetzt

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Krisenstab eingerichtet
- Datensicherungen zum Schutz gegen versehentliche Zerstörung und Datenverlust
- Wo notwendig: Nutzung redundante Systeme (z.B. NAS)
- Auswahl von Rechenzentrums-Anbieter aufgrund von Gütekriterien (z. B. ISO-27001)

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

Datenschutz-Management

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Datenschutzbeauftragter ist benannt
- Etablierung einer Datenschutzorganisation
- Alle Mitarbeitenden sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen
- Mitarbeitende sind im Umgang mit personenbezogenen Daten sensibilisiert
- Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Notfallmanagement
- Krisenstabsorganisation & Rollenkarten

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den Vertragszweck erforderlich sind (siehe Anlage 7: Pflicht- und optionale Felder)
- Es wird prozessual sichergestellt, dass die KODE® Produkte datenschutzfreundlich gestaltet werden
- Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Der Auftragnehmer erfüllt diesen Anspruch durch nachfolgend beschriebene Maßnahmen:

- Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt
- Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers unter Vorhandensein einer Auftragsvereinbarung verarbeitet

Besondere technische und organisatorische Maßnahmen für 1und1 IONOS-Rechenzentren / Applikationsserver für KODE®/KODE®X

Anwendbarkeit

Diese TOMs kommen zur Anwendung, wenn

- KODE®/KODE®X-Verfahren mit Onlinefragebögen zum Einsatz kommen

Rechenzentrum

Rechenzentren von 1und1 IONOS sind nach dem ISO 27001 Standard zertifiziert

- Selbstauskunft des Hosters: Elektronische Zutrittskontrollsysteme überwachen und gewährleisten den Zutritt zum jeweiligen Rechenzentrum nur für autorisierte Personen
- Sicherheitsschleuse
- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
- Definierte Sicherheitszonen
- Hochredundante Netzwerkinfrastruktur
- Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr
- Kühlsystem im Rechenzentrum / Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Keine sanitären Anschlüsse im oder oberhalb von Rechenzentren
- Alarmmeldung bei unberechtigtem Zutritt zu Rechenzentren

KODE®/KODE®X-Verarbeitung im Rechenzentrum (nachfolgend „KODESERVER“)

Der **KODESERVER** kann optional genutzt werden, um

- E-Mail-Notifications an Selbst- oder Fremdeinschätzer zu senden, die einen KODE®- und/oder KODE®X-Fragebogen ausfüllen sollen
- Fragebögen zu erfassen
- in Fällen serverbasierter Auswertungen: die Auswertungen dazu zu erzeugen
- Notification an prozessbeteiligte Person, damit diese über die Fertigstellung eines Fragebogens informiert wird

Folgende Maßnahmen sind auf dem KODESERVER implementiert

- Hinweis an die Anwendenden vor der Erfassung, dass Daten erfasst werden und welche Daten erfasst werden („Datenschutz“ muss jedes Mal aktiv zum Fragebogenbeginn bestätigt werden)
- Datenminimalismus (z. B. keine Mandantenzugehörigkeit und keine Personennamen bei Selbst-Einschätzungen) auf dem Server
- Daten in Serverdatenbank sind AES 256 verschlüsselt
- Rollenfestlegungen für Updates (Servers, Web-App, Datenbank-Server)
- Daten nach Klick auf „Abschließen“ nicht mehr veränderbar
- automatische Löschung von Log-Files (Webserver, KODE®-WebApp-Logs) nach 60 Tagen
- tägliche Datensicherung (sichert gegen Gesamt-Datenbank-Ausfall)
- automatische Löschung der Datenbanksicherung nach 15 Tagen
- Datenübertragung zwischen Anwendenden und KODE®-Server verschlüsselt (https)
- AV-Vertrag mit Rechenzentrum 1und1 IONOS liegt vor

Besondere technische und organisatorische Maßnahmen für AZURE-Rechenzentren

Anwendbarkeit

KODE® Cloud Produktivsystem

KODE® Cloud Entwicklungssystem

KODE® Cloud Testsystem (insofern für Kunden bereitgestellt!)

Informationen zu technischen und organisatorischen Maßnahmen sowie dessen Zertifizierungen sind auf der Anbieter-Internetseite hinterlegt:

Standort: Microsoft Azure Cloud (Westeuropa)

EU Cloud Code of Conduct

(Verhaltensregeln nach Art. 40 DSGVO, die bestätigt, dass Dienstanbieter konform zum europäischen Datenschutzrecht arbeitet)

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-eu-cloud-coc>

ISO/IEC 27001:2013 Information Security Management Standards

ISO/IEC 27017:2015 Verhaltenskodex für Informationssicherheitskontrollen

<https://docs.microsoft.com/de-de/compliance/regulatory/offering-ISO-27018?view=o365-worldwide>

[abgerufen am 28.06.2022]

ISO/IEC 27018-Verhaltenskodex zum Schutz von personenbezogenen Daten in der Cloud

<https://docs.microsoft.com/de-de/compliance/regulatory/offering-iso-27017?view=>

[abgerufen am 28.06.2022]

System- und Organisationskontrollen (SOC1 bis SOC3)

<https://docs.microsoft.com/de-de/compliance/regulatory/offering-soc-1?view=o365->

[worldwide](#)

<https://docs.microsoft.com/de-de/compliance/regulatory/offering-soc-2?view=o365-worldwide>

<https://docs.microsoft.com/de-de/compliance/regulatory/offering-soc-3?view=o365-worldwide> [abgerufen am 28.06.2022]