Auftragsverarbeitungs-Vertrag

nach Art. 28 Abs. 3 DS-GVO

zwischen

Kunde (der Vertragspartner der olmogo GmbH im Hauptvertrag zum Erwerb eines olmogo Produktes)
bzw.:

Kunde
Straße
Ort

im Folgenden ‘Auftraggeber’ genannt

und

olmogo GmbH
Landshuter Allee 8
80637 München

im Folgenden ‘Auftragnehmer’ genannt

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Auf Basis dieses Auftragsverarbeitungs-Vertrages erfolgt eine Verarbeitung von personenbezogenen Daten nach Art. 28 DS-GVO. Durch den Auftraggeber beauftragt wird Bereitstellung und Betrieb von Softwarelösungen, die der Datenspeicherung und der Kommunikation über das Internet dienen. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in der Schweiz erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein hier nicht eingeschlossenes Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheits-Beschluss der Kommission, Standard Datenschutzklauseln, genehmigte Verhaltensregeln).

Diese Vereinbarungen stellen keine Standardvertragsklauseln im Sinne von Art. 28 Abs. 8 DS-GVO dar.

Dauer des Auftrags

Der Auftraggeber hat regelmäßig einen Hauptvertrag über die Nutzung von olmogo Produkten geschlossen. Dauer, Kündigungsfrist und mögliche Kündigungstermine dieses Vertrages entsprechen dem Hauptvertrag. Ansonsten wird dieser Vertrag auf unbestimmte Zeit geschlossen und die Kündigungsfrist ist 30 Tage.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die durch den Hauptvertrag zur Nutzung von olmogo Produkten beauftragen Leistungen sowie sonstige im Hauptvertrag enthaltene Vereinbarungen bestimmen Zweck, Art, Umfang der Erhebung, Verarbeitung, Nutzung personenbezogener Daten.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO)

Die Art der Verarbeitung besteht regelmäßig in den Vorgängen Erheben/Erfassen, Ordnen/Sortieren/Organisieren, Speichern, Bereitstellen, Löschen/Einschränken von Daten.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO)

Typische Datenarten sind:

- Quell-/Nutzdaten, z.B. Files aller Art, Datenströme, insbesondere auch Audio-/Video Streams, temporäre Speicherinhalte, Signaturdatei, Bildschirminhalte bei Screen-Sharing, Dokumente, E-Mails und sonstige Arten von Nachrichten
- Stammdaten von Personen, z.B. Name, Adresse, Anrede
- elektronische Adressdaten, z.B. Telefonnummer, Faxnummer, E-Mail-Adresse
- Daten aus und zu Verträgen mit dem Auftraggeber, z.B. Vertragsabschluss, textliche Aufzeichnungen zu Anfragen des Vertragspartners
- Support Daten z.B. Textkommunikation und textliche Aufzeichnungen zu Supportanfragen
- Nutzungsstatistiken, Cookies und vergleichbare Technologien
- Daten bezüglich Zahlungsvorgängen
- Einträge technischer Logs, diese können Rückschlüsse auf u.a. Arten und Zeitpunkte von Interaktionen des Nutzers mit den Systemen zulassen

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO)

Typische Kategorien betroffener Personen sind:

- Kunden
- Personen denen der Kunde die Nutzung der erworbenen olmogo-Produkte ermöglicht, wie z.B. Mitarbeiter oder Familienmitglieder des Kunden
- Kunden von Kunden, Kommunikationspartner von Kunden (z.B. Mandanten, Empfänger/Sender von Nachrichten/Dateien/Kommunikations-Streams)
- Interessenten für olmogo-Produkte
- Mitarbeiter von olmogo
- Geschäftspartner von olmogo und deren Mitarbeiter
- Vertriebs-/Technologiepartner von olmogo und deren Mitarbeiter

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
Änderungen des Verarbeitungs-Gegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftrags-Ergebnisse feststellt.
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.

4. Für Weisung zu nutzende Kommunikationskanäle

Postalisch:
olmogo GmbH
Landshuter Allee 8
80637 München

Telefon: +49 89 61422000
E-Mail: solution@olmogo.com

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutz Behörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen von dieser Regelung sind Sicherheitskopien, welche für die korrekte Durchführung des Betriebes notwendig sind.

Der Auftragnehmer sichert im Bereich des Auftrags gemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Der Auftragnehmer prüft durch regelmäßige Kontrollen die Einhaltung der festgesetzten technischen und organisatorischen Maßnahmen u.a. mit dem Ziel der Prüfung und Sicherstellung der Einhaltung geltenden Datenschutzrechts und des Schutzes von Rechten und Daten. Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungs-Tätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer

im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (z.B. bei Tele- bzw. Heimarbeit von Mitarbeitern des Auftragnehmers) ist gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutz-Regeln zu beachten, die dem Auftraggeber obliegen: Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B.

Angemessenheits-Beschluss der Kommission, Standard Datenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Zurzeit sind für den Auftragnehmer die in

Anlage 1 – Subunternehmer

mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Eine derartige Information erfolgt spätestens 30 Tage vor der geplanten Übertragung der Daten an den neuen Subunternehmer. Die Information erfolgt in Schriftform/Textform. Die Hinzuziehung/ Ersetzung ist zulässig, falls der Auftragnehmer nicht bis spätestens 14 Tage vor der geplanten Übertragung Einspruch erhebt. Im Falle eines derartigen Einspruchs steht dem Auftragnehmer ein außerordentliches Kündigungsrecht zu. Dieses betrifft sowohl diesen Vertrag wie auch geschlossene Hauptverträge zur Nutzung etc. von olmogo-Produkten. Ansprüche des Auftraggebers auf Schadensersatz sind dabei ausgeschlossen.

8. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder

Nutzungs-Ergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

9. Haftung

Auf Art. 82 DS-GVO wird verwiesen.

10. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

München, den , den

_____ _____

Auftragnehmer Auftraggeber

Anlage 1 – Subunternehmer

- Sparkasse Oberland, Marienplatz 2-6, 82362 Weilheim: Zahlungsdienstleister
- domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning: Daten für Kundenverträge, Kundenkommunikation
- Infomaniak Network SA, Rue Eugène-Marziano 25, 1227 Genève - Schweiz: Daten für Kundenverträge, Kundenkommunikation, Betrieb der Webseite und Verarbeitung dabei anfallender Daten
- Deutsche Telekom AG, Friedrich-Ebert-Allee 140, 53113 Bonn: Backend für Funktionen der Software olmogo S3/M3

Anlage 2 – technisch und organisatorische Maßnahmen

Dieses Dokument beschreibt die technisch organisatorischen Maßnahmen (TOM) der olmogo GmbH, Landshuter Allee 8, 80637 München, die betrieben werden, um einen optimalen Schutz aller Kundendaten und personenbezogener Daten sicherzustellen.

Zutrittskontrolle

Maßnahmen, die verhindern, dass die Datenverarbeitungseinrichtungen durch unbefugte genutzt werden können:
Die Daten der Services, den die olmogo GmbH anbietet liegen in der Open Telekom Cloud (OTC) der deutschen Telekom. Die Rechenzentren sind über einen vier Meter hohen Erdwall gegen Brachial-Angriffe, zwei Meter hohe Sicherheitszäune mit Stacheldraht und mehr als 300 Überwachungskameras und Bewegungsmelder geschützt. Im Inneren wird dieses Konzept mit Sicherheitsschleusen und Handscannern konsequent fortgesetzt. In die Serverräume gelangt man sogar nur über eine zusätzlich gesicherte Hochbrücke. Gut ausgebildetes Sicherheitspersonal bewacht den gesamten Campus rund um die Uhr.

Zugangskontrolle

Maßnahmen, dass Clientrechner von unbefugten Personen genutzt werden können:
Alle Client Rechner der Mitarbeiter der olmogo GmbH sind über ein sicheres Passwort und/oder über eine biometrische Nutzerkennung gesichert. Die Clients sperren sich automatisch nach kurzer Nichtbenutzung. Sensible Daten sind auf den Datenträgern nochmals speziell verschlüsselt und somit vor unbefugtem Zugriff zusätzlich geschützt. Code Signing Zertifikate sind auf externer Hardware (USB-Tokens etc.) gespeichert.
Der Zugriff auf die Cloud Infrastrukturen der OTC ist nur wenigen Mitarbeitern möglich und neben hoch starken Passwörtern zusätzlich mit Zertifikaten abgesichert, die regelmäßig erneuert bzw. ausgetauscht werden.

In den Rechenzentren der Telekom dienen eine Firewall, sowie unterschiedliche Intrusion-Detection-Systeme, die Datenströme auf verdächtige Bestandteile wie Schadcodes untersuchen als Schutzmaßnahmen. Verschiedene Verschlüsselungstechniken sorgen dafür, dass die sensiblen Daten der Kunden nur von autorisierten Telekom Mitarbeitern eingesehen werden können. Außerdem stehen weltweit über 1.000 Sicherheitsexperten im Telekom-Konzern im permanenten Austausch, um sämtliche Systeme stetig weiterzuentwickeln. Ein spezielles Cyber Defense Team beschäftigt sich rund um die Uhr mit der Erkennung und Vorbeugung von Angriffsmustern. Das Cyber Emergency Response Team kann bei Bedarf nahtlos in den Prozess eingreifen und auf etwaige oder erfolgte Hackerangriffe reagieren.
Sogar über die strengen Vorgaben der DS-GVO hinaus ist die Open Telekom Cloud nach dem Trusted Cloud Datenschutz Profil (TCDP) 1.0 zertifiziert. Damit ist sie beinahe ein

einzigartiges Angebot am Markt, welches über eine rechtskonforme Datenschutz Zertifizierung für Cloud-Dienste verfügt.
Weitere Zertifizierungen der Telekom Cloud können unter https://open-telekom-cloud.com/de/sicherheit/datenschutz-compliance eingesehen werden.

Zugriffskontrolle

Maßnahmen, die sicherstellen, dass insbesondere personenbezogene Daten nur von Personen mit der entsprechenden Berechtigung zugreifbar sind und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können:
Alle Daten sind nach Technik, Vertrieb und Entwicklung klassifiziert und die Zugriffe durch ein Berechtigungskonzept geregelt. Insbesondere Datenschutz relevante personenbezogene Daten sind auf einer separaten Cloud mit eigens eingerichtetem Zugriffsmanagement innerhalb des CRM-Systems abgelegt.
Das CRM-System wiederum ist mit Mitarbeiterbezogenen Zugängen und Passwörtern geschützt. Das Anlegen und Verändern von Daten wird mit Nutzernamen und Zeitpunkt mitgeloggt. Die Berechtigungskonzepte stellen sicher, dass nur definierte Mitarbeiter Zugriffe auf personenbezogene Daten haben.

Weitergabekontrolle

Maßnahmen, die sicherstellen, dass Daten während dem Transport oder während der Speicherung nicht von unbefugten gelesen, kopiert, verändert oder entfernt werden können:
Bei der Übermittlung personenbezogener Daten an Dritte werden jeweils gesonderte Vereinbarungen oder AVVs mit diesen dritten Parteien geschlossen. Die olmogo GmbH ist sehr darauf bedacht den korrekten und DS-GVO konformen Umgang mit Daten auch bei seinen Dienstleistern sicherzustellen und wählt diese entsprechend kritisch und nach strengen Maßstäben aus.
Daten werden immer nur verschlüsselt übertragen bzw. transportiert.

Eingabekontrolle

Maßnahmen, die sicherstellen, dass nachvollzogen werden kann, wann und von wem personenbezogene Daten eingegeben bzw. verändert worden sind:
Personenbezogene Daten werden immer mit einer Zuständigkeit, einem Ersteller, einem Änderungsdatum und einem letzten Bearbeiter dokumentiert.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur analog den Weisungen des Auftraggebers verarbeitet werden können:
Auftragsverarbeitungen im Sinne von Art. 28 DS-GVO erfolgen nur entsprechend Weisungen des Auftraggebers und den Maßgaben der relevanten Auftragsverarbeitungs-Verträge. Mit Auftragsverarbeitungen befasste Mitarbeiter verfügen über entsprechende Kenntnisse bzw. werden entsprechend geschult, um die Kenntnisse aufzubauen. Dienstleister, bei denen
die olmogo GmbH als Auftraggeber eine Auftragsdatenverarbeitung auftritt werden streng ausgewählt. Bei Notwendigkeit werden Maßnahmen ergriffen, um den korrekten Umgang der Auftragnehmer mit Daten sicher zu stellen, wie z.B. Kontrollen oder ein Wechsel des beauftragten Datenverarbeiters.

Verfügbarkeitskontrolle

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

Es erfolgen regelmäßige Datensicherungen. Dabei werden zunächst vom jeweiligen Dienstanbieter konfigurierte und durchgeführte Backup Mechanismen und sonstige relevante technische Maßnahmen eingesetzt. Auf Grund der Auswahl von Anbieter und Tarifen haben diese Verfahren eine hohe Qualität. Zusätzlich werden durch die olmogo GmbH konfigurierte Backup Mechanismen verwendet, welche das Sicherheitsniveau in besonders kritischen Bereichen nochmals erhöhen.

Trennungsgebot

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

Die für unterschiedliche Zwecke benötigten Daten werden auf getrennten IT-Systemen, teilweise verschiedener Anbieter, gehostet. Der Zugang erfolgt entsprechend mit getrennten Zugangskonten.

Datenschutzfreundliche Voreinstellungen

Die olmogo GmbH erhebt intern nur in dem Umfang personenbezogene Daten, wie es zum jeweiligen Zweck unbedingt erforderlich ist.
Alle Grundeinstellungen innerhalb der Systeme von olmogo sind maximal auf den Schutz aller Kunden- und personenbezogenen Daten ausgelegt.