360dialog Datenverarbeitungsvertrag nach Art. 28 GDPR ("DPA")

Diese DPA ist **Anhang 1** der Vereinbarung zwischen den Parteien

der "Hauptvertrag"), wobei

der Klient der Auftraggeber (Controller) und **360dialog GmbH** der Auftragsverarbeiter (Prozessor) ist, und tritt an dem Tag in Kraft, an dem sowohl die Hauptvereinbarung als auch diese DPA von allen Parteien ordnungsgemäß unterzeichnet werden.

Die in der Datenschutz-Grundverordnung verwendeten und definierten Begriffe haben in dieser DPA dieselbe Bedeutung.

Nur der englische Vertragstext ist bindend, die deutsche Übersetzung dient ausschließlich zu Informationszwecken. Beachten Sie bitte, dass im Falle eines Rechtsstreits ausschließlich die offizielle englische Fassung dieses Dokuments gilt.

1 Einzelheiten der Verarbeitung

1.1 Der Auftraggeber kann dem Auftragsverarbeiter personenbezogene Daten übermitteln, oder der Auftragsverarbeiter kann Zugang zu personenbezogenen Daten des Auftraggebers haben, während die Parteien den Hauptvertrag durchführen. Einzelheiten zu den verarbeiteten Datenkategorien, den betroffenen Personen und der Art der Verarbeitung sind in **Anhang DPA1** beschrieben.

1.2 Die personenbezogenen Daten werden für die Zwecke und die Dauer des Hauptvertrags verarbeitet.

2 Controller Verantwortung

Im Rahmen des Hauptvertrags ist der Auftraggeber allein für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre verantwortlich, insbesondere hinsichtlich der Offenlegung und Übermittlung personenbezogener Daten an den Auftragsverarbeiter und der Verarbeitung personenbezogener Daten, Art. 28 III 1 GDPR.

3 Pflichten des Verarbeiters

3.1 Der Auftragsverarbeiter darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten, Art. 28 III 2, lit. a) GDPR. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung der verantwortlichen Stelle gegen das Datenschutzrecht verstößt, hat er die verantwortliche Stelle unverzüglich zu informieren, Art. 28 III 3 DSGVO.

3.2 Der Auftragsverarbeiter trifft die geeigneten technischen und organisatorischen Maßnahmen, um personenbezogene Daten angemessen gegen die zufällige oder unrechtmäßige Zerstörung, den Verlust, die Veränderung, die unbefugte

Weitergabe oder den unbefugten Zugang zu personenbezogenen Daten gemäß Art. 28 III 2, lit. c), Art. 32 GDPR, beschrieben in **Anhang DPA2.**

3.3 Der Auftragsverarbeiter stellt sicher, dass alle Mitarbeiter, die der Auftragsverarbeiter zur Verarbeitung personenbezogener Daten in seinem Namen ermächtigt, zur Vertraulichkeit in Bezug auf diese personenbezogenen Daten verpflichtet werden. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung dieser DPA fort, Art. 28 III 2 lit b) DSGVO.

3.4 Der Auftragsverarbeiter benachrichtigt den Auftraggeber unverzüglich, nachdem er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat, Art. 33 II DSGVO. Auf Ersuchen des Auftraggebers leistet der Auftragsverarbeiter dem Auftraggeber unverzüglich jede angemessene Unterstützung, die erforderlich ist, damit derAuftraggeber die zuständigen Behörden und/oder die betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten unterrichten kann, sofern der für die Verarbeitung Verantwortliche nach dem Datenschutzgesetz dazu verpflichtet ist.

3.5 Außer in dem Umfang, der zur Einhaltung des geltenden Rechts erforderlich ist, wird der Auftragsverarbeiter nach Beendigung oder Ablauf dieser DPA alle personenbezogenen Daten (einschließlich Kopien davon), die gemäß dieser DPA und Artikel 28 III 2 lit g) DSGVO verarbeitet wurden, löschen oder zurückgeben. Sollte der Auftragsverarbeiter aus technischen oder anderen Gründen nicht in der Lage sein, personenbezogene Daten zu löschen, wird er Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten für eine weitere Verarbeitung gesperrt werden.

3.6 Der Auftragsverarbeiter wird es dem Auftraggeber ermöglichen, die Rechte der betroffenen Person gemäß Kapitel III der DSGVO (Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruchsrecht sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit zu erfüllen und dem Auftraggeber alle erforderlichen Informationen zur Verfügung zu stellen, Art. 28 III 2 lit e) DSGVO.

3.7 Der Auftragsverarbeiter unterstützt denAuftraggeber bei der Erfüllung der in den Artikeln 32 bis 36 DSGVO festgelegten Pflichten (Datensicherheitsmaßnahmen, Meldung von Datenschutzverletzungen an die Aufsichtsbehörde, Benachrichtigung der von einer Datenschutzverletzung betroffenen Personen, Datenschutz-Folgenabschätzung, vorherige Konsultation), Art. 28 III 2 lit f) DSGVO.

4 Prüfungen

4.1 Der Auftragsverarbeiter stellt dem Auftraggeber in Übereinstimmung mit den Datenschutzgesetzen und auf eine angemessene schriftliche Anfrage des Verantwortlichen hin die Informationen zur Verfügung, die sich im Besitz oder unter der Kontrolle des Auftragsverarbeiters befinden und die sich auf die Einhaltung der datenschutzrechtlichen Verpflichtungen des Auftragsverarbeiters in Bezug auf die Verarbeitung personenbezogener Daten beziehen, Art. 28 III 2 lit h) GDPR.

4.2 Gemäß Art. 28 III 2 lit. h) DSGVO kann der Auftraggeber auf schriftlichen Antrag und mit einer Vorankündigung von mindestens 30 Tagen an den Auftragsverarbeiter während der üblichen Geschäftszeiten und ohne Unterbrechung des Geschäftsbetriebs des Auftragsverarbeiters eine Inspektion des Geschäftsbetriebs des Auftragsverarbeiters durchführen oder durch einen qualifizierten Drittprüfer durchführen lassen, sofern der Auftragsverarbeiter seine Zustimmung erteilt hat, die nicht unbillig verweigert werden darf.

4.3 Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber auf dessen schriftliches Ersuchen hin mit einer Frist von mindestens 30 Tagen alle für eine solche Prüfung erforderlichen Informationen zur Verfügung zu stellen, soweit sich diese Informationen im Einflussbereich des Auftragsverarbeiters befinden und der Auftragsverarbeiter nicht durch geltendes Recht, eine Vertraulichkeitsverpflichtung oder eine sonstige Verpflichtung gegenüber einem Dritten an der Offenlegung gehindert ist.

5 Ort der Datenverarbeitung

Die gesamte Datenverarbeitung durch den Auftragsverarbeiter findet ausschließlich innerhalb der EU / des EWR statt, es sei denn, es wird für bestimmte Zwecke oder Funktionen in **Anhang DPA2** ausdrücklich etwas anderes angegeben**.** Im letzteren Fall stellt der Auftragsverarbeiter sicher, dass die Daten in Übereinstimmung mit Art. 45, 46 GDPRverarbeitet werden.

6 Unterauftragsverarbeiter

6.1 Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter mit Zustimmung des Auftraggebers gemäß Art. 28 II, III 2, lit. d), IV GDPR. Jeder Wechsel eines solchen Unterauftragsverarbeiters muss dem Auftraggeber gemeldet werden. Die Unterauftragsverarbeiter sind in **Anhang DPA3** aufgeführt**.**

6.2 Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter, so schließt er mit diesem einen Vertrag ab, der dem Unterauftragsverarbeiter dieselben Verpflichtungen auferlegt, die für den Auftragsverarbeiter gemäß dieser DSGVO gelten. Kommt der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen nicht nach, bleibt der Auftragsverarbeiter gegenüber dem Auftraggeber für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters haftbar.

6.3 Im Falle der Beauftragung eines Unterauftragsverarbeiters muss dem Auftraggeber Verantwortlichen das Recht eingeräumt werden, die Tätigkeiten des Unterauftragsverarbeiters gemäß diesem DPA und dem Datenschutzgesetz zu überwachen und zu überprüfen, einschließlich des Rechts, auf schriftlichen Antrag vom Auftragsverarbeiter Informationen über den Inhalt des Vertrags und die Umsetzung der Datenschutzverpflichtungen im Rahmen des Unterauftragsverarbeitungsvertrags zu erhalten, erforderlichenfalls durch Einsichtnahme in die einschlägigen Vertragsunterlagen.

7 Ansprechpartner, Datenschutzbeauftragter

Der Auftragsverarbeiter hat einen Datenschutzbeauftragten mit den unter **Anhang DPA4 aufgeführten** Einzelheiten benannt**.** Der Auftragsverarbeiter informiert denAuftraggeber über jede Änderung in dieser Position.

Anhang DPA1

Kategorien der verarbeiteten Daten	Betroffene Person(en)
User Name	End User
Message Content	End User

Anhang DPA2

0 Datenschutzkonzept & Technische und organisatorische Maßnahmen (TOM)

in Übereinstimmung mit Art. 32 EU-GDPR

360dialog GmbH
Version 2.2

1 Übersicht

Dieses Datenschutzkonzept / diese TOMs regeln die Datenverarbeitung der 360dialog GmbH, Torstraße 61, 10119 Berlin, Deutschland. Dieses Unternehmen ist auch Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

Die 360dialog GmbH verpflichtet sich, alle personenbezogenen Daten, sowohl von Kunden als auch von Geschäftspartnern, Mitarbeitern und anderen Betroffenen, vertraulich zu behandeln.

- rechtmäßig, in gutem Glauben und auf transparente Weise,
- für einen bestimmten Zweck,
- richtig,
- nur im notwendigen inhaltlichen und zeitlichen Umfang zur Datenminimierung verpflichtet
- und sicher
- und um den betroffenen Personen die Ausübung ihrer Rechte zu ermöglichen.

360dialog betrachtet den Datenschutz als einen kontinuierlichen Verbesserungsprozess und ist bestrebt, die Einhaltung aller geltenden Anforderungen regelmäßig zu überprüfen und zu verbessern.

Technische und organisatorische Maßnahmen sollen sicherstellen, dass alle Organisationen, die selbst oder in ihrem Auftrag personenbezogene Daten nutzen, verarbeiten oder sammeln, die gesetzlichen Bestimmungen der DSGVO einhalten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere die Risiken, die sich aus der Zerstörung, dem Verlust oder der Veränderung, unabhängig davon, ob diese zufällig oder unrechtmäßig erfolgt, oder aus der unbefugten Weitergabe von oder dem unbefugten Zugang zu personenbezogenen Daten ergeben, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

2 Vertraulichkeit (Artikel 32 Absatz 1 Buchstabe b der DSGVO)

2.1 Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten

verarbeitet oder genutzt werden. Maßnahmen zur Zugangskontrolle können automatische Zugangskontrollsysteme, der Einsatz von Chipkarten und Transpondern, die Zugangskontrolle durch Pförtner und Alarmanlagen zur Sicherung von Gebäuden und Räumen sein. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Systeme müssen in abschließbaren Serverschränken geschützt werden. Darüber hinaus ist es ratsam, die Zugangskontrolle durch organisatorische Maßnahmen zu unterstützen (z.B. Dienstanweisungen, die das Abschließen der Büros bei Abwesenheit vorsehen).

Die folgenden Maßnahmen verhindern den unbefugten Zugang zu den Büros und Datenverarbeitungssystemen von 360dialog und den Serverstandorten.

2.1.1 Zugang zu den Büroräumen

Die Sicherheit des räumlichen Zugangs wird gewährleistet durch:

- Schlüssel / Schlüsselvergabe für Büros mit sensiblen Daten
- Besuchsregelung: Externen Personen ist der Zutritt zu den Büroräumen grundsätzlich nur nach vorheriger Anmeldung gestattet. Sie müssen während der gesamten Zeit von einem Mitarbeiter begleitet werden. Dies gilt nicht für regelmäßig wiederkehrende externe Personen (z. B. Reinigungspersonal von externen Reinigungsfirmen).

2.1.2 Zugang zu den Rechenzentren

Der Zugriffsschutz auf die Rechenzentren wird durch das jeweilige Rechenzentrum realisiert. Die beauftragten Rechenzentren haben alle einen entsprechend hohen Standard, der den Anforderungen entspricht, z.B.

- persönliches Zugangskontrollsystem mittels Schlüssel/Schlüsselvergabe, RFID-Kartenleser oder ähnlich sichere Verfahren - für einen kleinen, begrenzten Personenkreis.
- Einsatz von Bewegungs- und Einbruchsmeldern, Videoüberwachung.
- Redundante Speicherung von Zugriffsprotokollen.
- Engagiertes Sicherheitspersonal vor Ort.
- Besuchsregelung: Externe Personen dürfen die Büroräume grundsätzlich nur nach vorheriger Anmeldung und Genehmigung durch die Geschäftsleitung betreten. Sie müssen während der gesamten Zeit von einem Mitarbeiter begleitet werden. Dies gilt nicht für regelmäßig wiederkehrende externe Personen (z. B. Reinigungspersonal von externen Reinigungsfirmen).
- Google: Sicherheitskorridor, Fahrzeugsperren, Metalldetektoren, Zäune.
- 360dialog wählt Rechenzentren aus, die ihre Sicherheit durch entsprechende Audits oder Zertifizierungen (z.B. ECO-Audit 5-Sterne, DIN ISO/IEC 27001:2008-09 oder vergleichbar) nachgewiesen haben und somit die Anforderungen der DSGVO erfüllen.

2.2 Physische Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen, mit denen personenbezogene Daten

verarbeitet und genutzt werden. Möglichkeiten sind z.B. Boot-Passwort, Benutzeridentifikation mit Passwort für eingesetzte Betriebssysteme und Softwareprodukte, Bildschirmschoner mit Passwort, die Verwendung von Chipkarten zur Anmeldung sowie der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen erforderlich sein, um z.B. unberechtigte Zugriffe zu verhindern (z.B. Richtlinien für die Einrichtung von Bildschirmen, Herausgabe von Orientierungshilfen für die Nutzer zur Wahl eines "guten" Passwortes).

Grundsätzlich ist jeder Zugang zu personenbezogenen Daten zugriffsgeschützt.

Im Einzelnen sind die folgenden Zugriffe auf Daten möglich:

2.2.1 Zugang zu den Anwendungssystemen über eine Webschnittstelle (regelmäßige Nutzung)

Jeder Nutzer (360dialog-Mitarbeiter und alle vom Kunden freigegebenen Nutzer) muss sich für den Zugriff auf personenbezogene Daten authentifizieren - in der Regel durch einen Benutzernamen und ein Passwort. Der erforderliche Zugang wird von Auth0 (https://auth0.com/), einer Cloud-basierten Lösung für das Identitätsmanagement, verwaltet.

2.2.2 Zugang zu den Backend-Systemen (z. B. für administrative Aufgaben, Zugang normalerweise über SSH oder VPN)

- Die IT-Systeme sind durch Firewall-Systeme und IP-Whitelisting vor unbefugtem Zugriff geschützt. Alle Server erfordern eine Authentifizierung, in der Regel durch gespeicherte, benutzerbezogene verschlüsselte SSH-Schlüssel. Diese Schlüssel müssen eine Mindestschlüssellänge von 2048 Bit haben und passwortgeschützt sein. Der Zugriff auf Datenbanken ist über ein VPN nur nach erfolgreicher starker Authentifizierung am jeweiligen Server möglich, so dass der Schutz durch Benutzername und Passwort als ausreichend angesehen wird.
- Server-Management-Konsolen (iDRAC) sind nur über ein internes Netzwerksegment zugänglich.
- Es gibt ein IP-Whitelisting auf API-Ebene, um den Zugang nur für autorisierte Systeme zu ermöglichen.
- Auf den Arbeitsplätzen ist ein Bildschirmschoner mit Passwortschutz installiert.

2.3 Zugangskontrolle

Die Maßnahmen zur Zugriffskontrolle sind so zu gestalten, dass nur auf Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht, und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann u.a. durch geeignete Berechtigungskonzepte sichergestellt werden, die eine differenzierte Steuerung des Datenzugriffs ermöglichen. Dabei ist es wichtig, sowohl den Inhalt der Daten als auch die möglichen Zugriffsfunktionen auf die Daten zu differenzieren. Darüber hinaus sind geeignete Kontrollmechanismen und Zuständigkeiten zu definieren, um die Erteilung und den Entzug von Berechtigungen zu dokumentieren und aktuell zu halten (z.B. bei Einstellung, Stellenwechsel oder Beendigung des Arbeitsverhältnisses). Besonderes Augenmerk muss immer auf die Rolle und die Fähigkeiten der Administratoren gelegt werden.

2.3.1 Minimum an autorisierten Personen

Mit 360dialog wird die Zahl der Personen, die Zugang zu den oben genannten Datenverarbeitungsanlagen haben, auf ein Minimum reduziert. Wie in der Regelung der Zugangskontrolle beschrieben, wird zwischen folgenden Personengruppen unterschieden:

2.3.2 360dialog System- und Datenbankadministratoren

- Systemadministratoren können die von der Geschäftsleitung erteilten Zugangs- und Zugriffsberechtigungen in das System eingeben und entsprechende Berechtigungsmerkmale in protokollierter Form vergeben (z.B. SSH-Schlüssel), Systemwartungen und -aktualisierungen durchführen, Serverprotokolle einsehen und allgemein serverbezogene Verwaltungsaufgaben wahrnehmen.
- Datenbankadministratoren können sich direkt bei den jeweiligen Datenbanken und Tabellen auf Datenbankebene anmelden, um Verwaltungsaufgaben durchzuführen und Backups zu erstellen.
- Der Zugriff auf Datenbank- oder Betriebssystemebene ist nur für 360dialog-Mitarbeiter möglich.

2.3.3 360dialog-Entwickler und Integrationsspezialisten

- Entwickler und Integrationsspezialisten von 360dialog können für Wartung, Instandhaltung, Fehlersuche und Ursachenanalyse oder verwandte Arbeitsaufgaben auf Protokolldateien und Datenbanken zugreifen.
- Sie bedürfen der Zustimmung der Geschäftsleitung, die per Weisung an die Abteilungsleitung delegiert wurde. Der Personenkreis wird auch mit dem Auftraggeber abgestimmt.

2.3.4 Benutzer

- Innerhalb der Anwendungsebene gibt es verschiedene Benutzerrollen und Gruppen, die jeweils mit dem Mandanten abgestimmt sind. Hier können sowohl Nutzer des Mandanten als auch Mitarbeiter von 360dialog Zugriff haben. Normale Benutzer können sich nur über die jeweiligen Weboberflächen in die Anwendungssysteme einloggen und die ihren jeweiligen Zugriffsrechten entsprechenden Aufgaben wahrnehmen.
- Sobald ein Mitarbeiter aufgrund seines Ausscheidens aus dem Unternehmen oder seiner fachlichen Aufgabe den Zugang nicht mehr benötigt, wird sein persönlicher Zugang wieder gesperrt und die zugehörigen Daten unwiederbringlich gelöscht. Dies geschieht in der Regel durch periodische Kontrollen, auf Wunsch des Kunden oder bei Beendigung des Vertragsverhältnisses.

2.3.5 Passwort-Regeln

Die von 360dialog vergebenen Passwörter entsprechen den folgenden Richtlinien:

- eine Mindestlänge von 8 Zeichen, leere Passwörter sind nicht zulässig,

- ein Zeichenmix aus mindestens drei Kategorien: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen (!@#$%^&*)
- kein leicht zu erratender Begriff und kein triviales Passwort (aus einer Liste der 10.000 häufigsten Passwörter),
- keine Verwendung von historischen Passwörtern (die Historie kennt 10 Passwörter),
- kein Teil des Benutzernamens Teil des Passworts ist.

Benutzerpasswörter, die für Benutzer des Kunden bestimmt sind, werden entweder direkt vom Kunden vergeben oder von autorisierten Mitarbeitern von 360dialog gemäß den jeweiligen Passwortrichtlinien eingerichtet.

Einmal erstellte Passwörter müssen regelmäßig geändert werden (mindestens alle 6 Monate).

Das erste Passwort muss dem Nutzer auf sichere Weise übermittelt werden und/oder der Nutzer muss aufgefordert werden, es zumindest unmittelbar nach der ersten Anmeldung zu ändern. Wenn Benutzername und Passwort zur Authentifizierung erforderlich sind, wird das entsprechende Passwort niemals im Klartext auf dem Bildschirm angezeigt. Dies gilt für alle Zugriffsmöglichkeiten - ob über Webinterface, SSH-Zugang oder Datenbankzugriff, und ob durch Mitarbeiter von 360dialog oder autorisierte Nutzer des Kunden.

2.3.6 Passwortverwaltung

Die Anwendungspasswörter bei 360dialog werden über Passbolt Pro verwaltet, das auf einem dedizierten Rechner mit eigener Datenbank im Rechenzentrum gehostet wird. Die Anmeldedaten für die Infrastruktur werden über Hashicorp Vault verwaltet.

2.3.7 Sichere Übertragung von Authentifizierungsgeheimnissen (Credentials) im Netz

Alle Registrierungen, die über ein Netzwerk erfolgen, sind immer verschlüsselt. Bei webbasierten Benutzeroberflächen werden diese TLS / HTTPS verschlüsselt und über und als JSON Web Token (JWT) kodiert. Für den direkten Zugriff auf Server wird dieser optional über SSH oder VPN (IPSec, openVPN o.ä.) verschlüsselt.

2.3.8 Protokollierung des Zugangs

- Zugriffsversuche (sowohl erfolgreiche als auch abgewiesene) auf die Server auf SSH-Ebene werden in den Serverprotokollen gespeichert und 3 Monate lang aufbewahrt.
- Zugriffsversuche auf die Webinterfaces werden aufgezeichnet und in Auth0 (https://auth0.com/) protokolliert Auth0 Bei Brute-Force-Angriffen oder Passwortmissbrauch wird Auth0 aktiv und blockiert den Zugriff.

2.3.9 Verschlüsselung und Löschung von Daten

Gedruckte Projekt- und Vertragsunterlagen werden mit einem Schredder der Stufe 2 vernichtet.

2.3.10 Physische Löschung von Datenträgern

Alle Daten auf Laptops werden durch Festplattenverschlüsselung (z. B. FileVault) gesichert und bei Wiederverwendung der Geräte sicher gelöscht. Wenn Bürohardware verkauft oder Serverfestplatten an das Rechenzentrum zurückgegeben werden, werden die Datenträger physisch gelöscht und nach dem Zufallsprinzip beschrieben, um eine Rekonstruktion der ursprünglichen Daten zu verhindern.

Externe Datenträger werden nicht für die Sicherung, den Transport und die Speicherung verwendet.

2.4. Trennungskontrolle

Mit der Trennungskontrolle soll sichergestellt werden, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können. Dies kann z. B. durch eine logische und physische Trennung der Daten gewährleistet werden.

2.4.1 Gesonderte Verarbeitung

Die personenbezogenen Daten der jeweiligen Mandanten werden völlig getrennt voneinander verarbeitet und eindeutigen logischen, isolierten Datenbanktabellen zugeordnet. Eine Ausnahme bilden Puffer und Lookup-Tabellen, die gemeinsam genutzt werden, aber eine logische Mandantentrennung gewährleisten.

2.4.2 Trennung von Test- und Produktionssystemen

Test- und Produktionssysteme sind logisch voneinander getrennt.

2.4.3 Sparsamkeit bei der Datenerhebung

Der Kunde entscheidet selbst, ob und welche personenbezogenen Daten über die von 360dialog angebotenen Funktionen hinaus erhoben und verarbeitet werden.

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

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, ohne dass zusätzliche Informationen erforderlich sind, vorausgesetzt, diese zusätzlichen Informationen werden getrennt aufbewahrt und unterliegen geeigneten technischen und organisatorischen Maßnahmen.

2.5.1 Löschungsfristen statt Pseudonymisierung

Eine Pseudonymisierung wird nur auf Wunsch des Auftraggebers und nach vorheriger Absprache durchgeführt, da eine Pseudonymisierung historische Personalisierungsdaten unbrauchbar machen kann. Stattdessen werden Aufbewahrungsrichtlinien vereinbart und die Daten werden vollständig gelöscht.

2.5.2 Pseudonymisierung zu Auswertungszwecken

KPIs (=Key Performance Indicator) werden zu Auswertungszwecken historisch gespeichert. Es handelt sich dabei lediglich um Zähler, die einen bestimmten Zeitraum abbilden und deren Auflösung keine Rückschlüsse auf die Nutzer zulässt.

2.5.3 Pseudonymisierung vor der Übertragung

Eine interne Richtlinie regelt: Werden personenbezogene Daten aus dem Produktionssystem im Rahmen einer Analyse weitergegeben, werden sie pseudonymisiert, es sei denn, sie sind für die Darstellung des Sachverhalts von Bedeutung.

3 Integrität (Art. 32 Abs. 1 lit. b GDPR)

3.1 Kontrolle übertragen (Weitergabe der Kontrolle)

Mit der Weitergabekontrolle soll sichergestellt werden, dass personenbezogene Daten während der elektronischen Übermittlung oder während ihres Transports oder ihrer Speicherung auf einem Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es sollte möglich sein, zu überprüfen und festzustellen, wohin personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden sollen. Zur Sicherstellung der Vertraulichkeit bei der elektronischen Datenübermittlung können z.B. Verschlüsselungstechniken und virtuelle private Netze eingesetzt werden. Maßnahmen für den Datenträgertransport oder die Datenübermittlung sind Transportbehälter mit Schließvorrichtungen und Regelungen zur datenschutzgerechten Vernichtung von Datenträgern.

3.1.1 Übertragung innerhalb der Systeme

Die Daten werden in der Regel über dedizierte Datenleitungen übertragen, zumindest aber verschlüsselt über ein VPN mit IP-Whitelisting.

3.1.2 Übermittlung an externe Systeme

- Alle APIs sind nur über HTTPS zugänglich.
- Es werden keine Daten an externe Systeme übertragen, es sei denn, dies ist ausdrücklich vereinbart. In diesen Fällen werden die Daten ausschließlich über sichere und verschlüsselte Kanäle übertragen.
- Sollte eine Übertragung notwendig werden, wird in der Regel SFTP mit Benutzername/Passwort (gemäß den Richtlinien) verwendet. Der Datenzugriff auf APIs oder über Webhooks erfordert Benutzernamen/Passwort (gemäß den Richtlinien). Die Protokollierung erfolgt über die SFTP-Serverprotokolle. Bei regelmäßigen Datentransporten an ein und denselben Empfänger werden sogenannte Schlüsseldateien (GPG) ausgetauscht, was die (separate) Übermittlung eines Passwortes überflüssig macht.
- Die Übermittlung auf elektronischen Datenträgern (USB-Sticks, mobile Festplatten, Notebooks, Smart Devices) ist nicht zulässig und bedarf in besonderen Fällen der ausdrücklichen Zustimmung der Geschäftsführung und des Auftraggebers.
- Auf den Arbeitsplätzen von 360dialog selbst werden keine personenbezogenen Daten dauerhaft gespeichert, sondern diese können temporär auf den jeweiligen Monitoren eingesehen werden.

3.1.3 Risikominimierung durch Netzwerktrennung

- Alle 360dialog-Server befinden sich hinter den entsprechenden Gateways bestehend aus Router und Firewall, der Zugriff auf die

Systeme kann nur über diese Gateways erfolgen. Die Gateways weisen Verbindungen ab, die aus einem nicht explizit freigegebenen Netz kommen. Für die 360dialog-Plattform gibt es eine physische Trennung von internen und externen Verbindungen über separate Netzwerksegmente (Drittsysteme wie WhatsApp können sich in anderen Rechenzentren befinden).

3.1.4 Umgang mit E-Mails

Personenbezogene Daten dürfen nicht per E-Mail übermittelt werden. In Ausnahmefällen und nach ausdrücklicher Vereinbarung mit dem Auftraggeber können komprimierte und verschlüsselte Dateien verwendet werden, sofern es sich um eine einmalige Angelegenheit handelt. Die Mitarbeiter müssen hierfür die Genehmigung ihres Vorgesetzten einholen.

3.1.5 Dokumentation

Die Datenempfänger, die Dauer der geplanten Übermittlung und die Löschungsfristen werden gemäß den Vorgaben der jeweiligen DSGVO oder dieser TOMs umgesetzt.

3.2 Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass die genauen Umstände der Dateneingabe nachträglich überprüft und festgestellt werden können. Die Eingabekontrolle wird durch eine Protokollierung erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) erfolgen kann. Es muss auch geklärt werden, welche Daten protokolliert werden, wer Zugriff auf die Protokolle hat, von wem und zu welchem Anlass/Zeitpunkt sie kontrolliert werden, wie lange sie aufbewahrt werden müssen und wann die Protokolle gelöscht werden.

3.2.1 Protokollierung

- Zugriffe von Systemadministratoren werden nur insoweit protokolliert, als ihre jeweiligen Anmeldeverfahren und die von ihnen gestarteten Befehle auf den Server-Shells aufgezeichnet werden. Alle anderen Befehle (z. B. in grafischen Konsolen gestartete Befehle) werden nicht aufgezeichnet. Für die erfassten Befehle wird eine Historie von 1000 Befehlen und für die Anmeldevorgänge eine Historie von 3 Monaten aufbewahrt. Der Zugriff der Systemadministratoren dient nicht der Verarbeitung oder dem aktiven Zugriff auf personenbezogene Daten, sondern der Pflege, Wartung und Aktualisierung der Serversysteme selbst.
- Zugriffe von Datenbankadministratoren werden nur insoweit protokolliert, als die von ihnen direkt in den Konsolenverwaltungsprogrammen eingegebenen Befehle aufgezeichnet werden und sie eine Historie von 1000 Befehlen führen. Werden grafische Verwaltungsprogramme verwendet, so werden die dort ausgeführten Befehle nicht aufgezeichnet. Der Zugriff der Datenbankadministratoren dient nicht der Bearbeitung oder dem aktiven Zugriff auf personenbezogene Daten, sondern der Pflege, Wartung und Aktualisierung der Datenbanken selbst.

3.2.2 Rückverfolgbarkeit/Protokollierung

Bei allen anderen (regelmäßigen) Nutzern, die die entsprechenden Anwendungsprogramme zur Verarbeitung personenbezogener Daten nutzen, wird der letzte Bearbeiter protokolliert. Die genaue Änderung selbst wird hier jedoch nicht erfasst. Sie kann im Einzelfall mit entsprechendem Aufwand abgeleitet werden.

3.2.3 Verantwortung für Löschungen

- Die Verantwortung für die Löschung liegt beim Eigentümer der jeweiligen Daten.
- Die Löschung von Daten in der Auftragsverarbeitung richtet sich nach dem jeweiligen DPA". Die Weisung wird vom berechtigten Personenkreis des Auftraggebers an die Projekt- oder Kundenverantwortlichen bei 360dialog übertragen. Jede Löschung bedarf einer schriftlichen Anweisung.

3.2.4 Löschung von Daten

- Live-Kommunikationsdaten werden mit der Zustellung an den Endempfänger gelöscht, spätestens jedoch sieben (7) Tage nach Erhalt.
- Alle anderen Daten werden gelöscht, wenn sie für den Zweck, für den sie ursprünglich verarbeitet wurden, nicht mehr benötigt werden.
- Vertragsdaten können in einigen Fällen bis zum Ablauf der gesetzlichen Verjährungsfristen für zivilrechtliche Ansprüche gespeichert werden. In diesem Fall werden die Daten außerhalb des Live-Systems gespeichert.
- Die Daten werden für die Dauer der gesetzlichen Aufbewahrungsfristen gespeichert. In diesem Fall werden die Daten außerhalb des Live-Systems gespeichert. Typische Aufbewahrungsfristen sind:

Die jährlichen Fristen enden immer am Ende des letzten Kalenderjahres.	Aufbewahrungsfrist	Rechtsgrundlage
Stundenzettel (allgemein)	2 Jahre	§ 16 Abs. 2 ArbZG
Bewerbungsunterlagen	bis zum Ablauf etwaiger Verjährungsfristen für Ansprüche	§ 15 Abs. 4 AGG, § 61 Abs. 1 ArbGG
DEÜV-Zertifikat über Datenübertragungen	bis zum Ende des auf den letzten Test folgenden Kalenderjahres	§ 25 DEÜV
Doppelbesteuerungsbescheinigung	6 Jahre	§ 39b Abs. 6 i.V.m. § 41 Abs. 1 EStG
Reisekostenerstattung	6 Jahre	§ 41 Abs. 1 EStG in Verbindung mit R 38 der Lohnsteuerrichtlinien
Infektionsschutzgesetz - Gesundheitszeugnis und Abschlussdokumentation der Belehrung.	bis zum Ausscheiden des Mitarbeiters aus dem Unternehmen	§ 43 Abs.. 5 IfSG
Lohnkonto (Steuer)	6 Jahre	§ 41 Abs.. 1 EStG

Lohnunterlagen (Sozialversicherung)	bis zum Ende des Kalenderjahres, das auf die letzte Prüfung folgt	§ 28f Abs.. 1 S. 1 SGB IV

3.2.5 Löschung von Daten auf Antrag

- Die Daten sind auf Antrag zu löschen, wenn die Voraussetzungen des Art. 17 GDPR erfüllt sind. Die Löschung hat in diesem Fall unverzüglich zu erfolgen.
- Im Zweifelsfall muss die betroffene Person, die die Löschung beantragt, durch geeignete Methoden authentifiziert werden.
- Im Falle eines solchen Antrags ist der DSB zu benachrichtigen.

4 Verfügbarkeit und Belastbarkeit (Art. 32 (1) lit (b) GDPR)

Mit der Verfügbarkeitskontrolle soll sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Datenverarbeitungssysteme sind "resilient", wenn sie so robust sind, dass ihre Funktionsfähigkeit auch bei starkem Zugriff oder starker Nutzung gewährleistet ist. Dies gilt nicht zuletzt im Hinblick auf die gezielte Überlastung von Servern, um die Verfügbarkeit trotz eines Angriffs von außen, zum Beispiel durch so genannte DoS- oder DDoS-Attacken ("Distributed Denial of Service"), zu gewährleisten. Dazu gehören auch Themen wie unterbrechungsfreie Stromversorgung, Klimatisierung, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz, RAID-Systeme, Plattenspiegelung etc.

4.1.1 Schutz des Serverraums

Serverräume haben die folgenden Merkmale:

- Brand- und Rauchmeldeanlagen
- Feuerlöscher im Serverraum
- Überwachung der Servertemperatur
- klimatisierter Serverraum
- UPS
- Steckdosenleisten zum Schutz
- Videoüberwachung
- Alarmmeldung bei unbefugtem Zutritt zum Serverraum

4.1.2 Redundante Bereitstellung von kritischen Systemen

Alle zentralen Funktionalitäten der Plattform werden redundant als vollwertiger Cluster oder Master-Slave-Konfiguration vorgehalten. Dies beinhaltet:

- Webserver
- Warteschlangen und Pufferspeicher
- Datenbanken und Schlüsselwertspeicher
- Geschäftslogik

Die Festplattensysteme sind zumindest mit einer grundlegenden Fehlertoleranz ausgestattet (RAID5 oder RAID6).

4.1.3 Sicherungskonzept

Um die Daten vor versehentlichem Verlust zu schützen, werden von diesen Daten Backups erstellt. Diese Backups werden verschlüsselt und getrennt von den Produktivdaten auf einem separaten Server im selben Rechenzentrum (auf Wunsch auch als weitere Kopie bei einem anderen Dienstleister)

gespeichert. Aufgrund der Verschlüsselung der Daten ist hier ein geringeres Schutzniveau für den physischen Zugriff angemessen - was jedoch keinen generellen Zugriff auf die dort befindlichen Datenverarbeitungssysteme und Datenträger erlaubt - da die Daten ohne entsprechende Berechtigung und Zugangsschlüssel nicht genutzt werden können.

Es werden keine Datensicherungen auf beweglichen, physischen Speichermedien wie Bändern oder CD-ROMs erstellt, und es besteht keine Notwendigkeit, die Speichermedien zu lagern.

Aufgrund des zentralen Datenhaltungsansatzes können unterschiedliche Sicherungsstrategien angewendet werden. Im Bereich der Datenbank werden mehrfach redundante Replikationen im Master/Slave-Betrieb sowie tägliche Sicherungen auf externe Datenträger durchgeführt. Dies ermöglicht im Falle eines Ausfalls des Datenbank-Masters ein schnelles Failover auf einen entsprechenden Slave-Server, ohne Datenverluste in Kauf nehmen zu müssen.

4.1.4 Schnelle Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c GDPR)

Für den Fall eines Anwendungs- oder Benutzerfehlers und dem damit verbundenen Datenverlust können Datenbank-Backups verwendet werden. Die Wiederherstellung erfolgt zeitnah gemäß dem definierten Service Level Agreement. Die Wiederherstellungsprozesse sind dokumentiert, so dass eine schnelle Reaktion möglich ist. Ersatzsysteme sind je nach Anforderung als Hot- oder Spareparts verfügbar

4.1.5 Getrennte Partitionen

Betriebssystem und Daten werden auf getrennten Festplatten gespeichert.

4.1.6 Notfallplan / Disaster Recovery

Der Ernstfall wird regelmäßig geübt. Im Falle einer Störung werden die entsprechenden Ansprechpartner auf Seiten des Kunden sofort informiert. Die Ansprechpartner sind in den Verträgen mit den Auftraggebern dokumentiert und werden bei Änderungen entsprechend aktualisiert.

4.1.7 Inspektion der Notfalleinrichtungen

Die regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzgeräten wird durch das von 360dialog beauftragte zertifizierte Rechenzentrum durchgeführt.

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

5.1 Datenschutz-Management

Das Unternehmen hat ein Datenschutzmanagementsystem (von ER Secure) eingeführt und mit

René Rautenberg,
ER Secure GmbH,
In der Knackenau 4,
82031 Grünwald

einen externen Datenschutzbeauftragten.

5.2 Schulungen, Rezensionen

- Dokumentation der einschlägigen Verarbeitung personenbezogener Daten, einschließlich regelmäßiger Aktualisierungen und Kontrollen
- Schulung und Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- Jährliche Sensibilisierung der Mitarbeiter
- Jährliche Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen
- Auskunfts- und Löschungsanträge gehen über privacy@360dialog.com und Schnittstellen ein und werden mindestens monatlich umgesetzt

5.3 Vorfall-Reaktions-Management

Die Plattform wird durch eine Firewall geschützt. fail2ban wird als Intrusion Prevention System (IPS) eingesetzt. E-Mail-Spam wird von der Spam-Filterung von GSuite Business erkannt und gefiltert.

5.3.1 Information und Eskalation

Sicherheitsvorfälle werden intern an den SysOp, den Solution Architect, den Head of Product und an die Geschäftsleitung gemeldet. Je nach Klassifizierung des Vorfalls wird auch der externe Datenschutzbeauftragte konsultiert oder der Kunde informiert, sofern er von dem Vorfall betroffen ist.

5.3.2 Dokumentation

In jedem Fall wird ein Ticket im Ticketsystem erstellt, in dem alle Informationen über den Vorfall und seine Lösung gesammelt werden. Die Abhilfemaßnahmen werden von den zuständigen Teamleitern akzeptiert und gegebenenfalls gegenüber dem Kunden ausgeführt.

5.4 Datenschutzfreundliche Voreinstellungen (Art. 25 (2) GDPR) / Privacy by Design, Privacy by Default

- Jeder Entwicklungsmitarbeiter wird über die Konzepte "Privacy by Design" und "Privacy by Default" informiert. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck notwendig sind. Die Umsetzung liegt in der Verantwortung des Mitarbeiters, die Kontrolle obliegt dem Head of Product und dem Solution Architect.
- Darüber hinaus werden personenbezogene Daten nur im Einvernehmen mit dem Kunden verarbeitet.
- Die Aufbewahrungsfristen werden so kurz wie möglich gewählt (30 oder 90 Tage). Ausnahmen werden mit dem Kunden vereinbart.

5.4.1 Ausübung des Widerrufsrechts

Betroffene können dem Tracking ihrer Daten widersprechen. Benachrichtigungen und Konversationen erfordern ohnehin die Zustimmung der Nutzer.

5.5 Auftragskontrolle

Ziel der Auftragskontrolle ist es, sicherzustellen, dass eine Auftragsdatenverarbeitung im Sinne des Art. 28 DSGVO ohne entsprechende

Weisung des Auftraggebers durchgeführt wird. Dieser Punkt umfasst neben der Datenverarbeitung im Auftrag des Auftraggebers auch die Durchführung von Wartungs- und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Soweit sich der Auftragnehmer im Sinne der Auftragsverarbeitung Dienstleistern bedient, sind die nachfolgenden Punkte stets mit diesen zu vereinbaren.

5.5.1 Umsetzung des Weisungsrechts

Der Datenzugriff durch autorisierte Nutzer wird darüber hinaus durch den Kunden selbst oder über den "Vertrag zur Auftragsverarbeitung gemäß Art. 28 GDPR", der von 360dialog erstellt und freigegeben wird.

5.5.2 Vorschriften/Einschränkungen bei der Auftragsabwicklung

Es dürfen nur Arbeiten ausgeführt werden, die in der zu erstellenden Leistungsbeschreibung enthalten sind. Alle darüber hinausgehenden Arbeitsschritte müssen im Vorfeld mit der zuständigen Stelle auf Seiten des Auftraggebers abgestimmt und schriftlich genehmigt werden. Der Auftragnehmer stimmt den Zeitplan für die Ausführung des Auftrages mit dem Auftraggeber im Voraus ab.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, vermuteten Datenschutzverletzungen, festgestellten Fehlern oder sonstigen Unregelmäßigkeiten im Umgang mit den Daten des Auftraggebers. Der Auftragnehmer wird diese unverzüglich beseitigen.

5.5.3 Unterauftragnehmer

Die Auswahl von Unterauftragnehmern erfolgt auf der Grundlage von festgelegten Sorgfaltskriterien und Sicherheitsmaßnahmen. Erforderliche Vereinbarungen zur Auftragsabwicklung oder EU-Standardvertragsklauseln werden getroffen. Das Weisungsrecht ist schriftlich festgelegt. Im Verdachtsfall wird der Unterauftragnehmer informiert und das Schutzniveau und die Datenvernichtung durch 360dialog überprüft.

Anlage

Partner und Schnittstellen

Die folgenden Schnittstellen können im jeweiligen Kontext verwendet werden. Weitere Details werden projektspezifisch definiert und dokumentiert.

1. Nachrichten-Gateways

Message Gateways liefern Nachrichten über die jeweiligen Datenverarbeiter aus:

- WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland

Sicherheitskonzept: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

2. Problemverfolgung

Produktentwicklung, Wartung, Zwischenfälle, Konfigurationseinstellungen, Datenverwaltungsaufgaben und Änderungen an Benutzern und Rechten werden über ein Problemverfolgungssystem dokumentiert.

- Atlassian Pty Ltd, c/o Atlassian, Inc., 350 Bush Street, San Francisco, CA 94104, USA

3. Hosting

In Betrieb genommene Rechenzentren (zum Zeitpunkt der Drucklegung dieses Dokuments) sind

1. Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland
2. Amazon Web Services EMEA SARL, avenue John F. Kennedy, L-1855, Luxemburg

Anhang DPA3

Unterauftragsverarbeiter 360dialog GmbH

Unternehmen/Auftragnehmer	Adresse/Land	Erbrachte Dienstleistung/Umfang
Google Irland Limited	Gordon House, Barrow Street, Dublin 4, Irland	GCP-Rechenzentrum/Hosting in Frankfurt, E-Mail-/App-Provider für die Kommunikation mit Kunden in Vertragsangelegenheiten und zur Kundenbetreuung. Personenbezogene Daten, wenn das WhatsApp-Gateway im GCP gehostet wird. Vertragsannahme per Klick.

Anhang DPA4

Technischer und administrativer Ansprechpartner für den Controller

support@360dialog.com
+49 30 609 859 530

Datenschutzbeauftragter

René Rautenberg,
René Rautenberg GmbH,
Radlkoferstr. 2,
81373 München, Deutschland,
+49.89.55294870,
info@er-secure.de